



FACULTAD DE CIENCIAS  
DEPARTAMENTO DE FÍSICA DE MATERIALES



CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS  
INSTITUTO DE SEGURIDAD DE LA INFORMACIÓN

# Design and Implementation of a High-Speed Free-Space Quantum Key Distribution System for Urban Scenarios

*Diseño e Implementación de un Sistema de  
Distribución Cuántica de Clave en Espacio Libre a Alta Velocidad  
para Escenarios Urbanos*

Tesis doctoral

María José García Martínez  
Ingeniera de Telecomunicación

Directora: Dra. Verónica Fernández Mármol

Tutor: Prof. Dr. José Manuel Calleja Pardo

Madrid, 2013



Este trabajo ha sido realizado en el marco de las becas predoctorales JAE de la Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), y parcialmente financiado por el proyecto TEC2012-35673.





To my parents, Pepe and Fina



## Agradecimientos

Me gustaría expresar mi más profundo agradecimiento a la directora de esta tesis, Dra. Verónica Fernández Mármol, por guiarme a través del fascinante mundo de la criptografía cuántica. Siempre le estaré agradecida por su trato personal y amistoso, y también por su gran esfuerzo y determinación al dirigir el grupo “cuántico”. También me gustaría agradecer al tutor de esta tesis, profesor Dr. José Manuel Calleja Pardo, por sus consejos y su apoyo inestimable.

Quisiera agradecer sinceramente a mis compañeros “cuánticos”, Natalia Denisenko y Diego Soto, que conocen de primera mano lo que ha costado poner el sistema en funcionamiento. Las largas horas en el laboratorio y las discusiones fructíferas han sido una gran experiencia y ayuda que realmente valoro. Gracias también a mis otros compañeros: Juanca (por tu tiramisú y tu trato encantador), Mari Carmen (tus cariñosos ánimos), Alfonso (tus cumplidos en el pasillo), Nacho (quiero el divorcio y me quedo con el cálculo de la división), Jesús (un gran fotógrafo pero mejor amigo). Gracias a mis queridos compañeros de fatigas, Alex (afortunado Alejandro, fue genial y muchas risas compartir mesa contigo; ¡vamos, tú puedes!) y Carmen (encantadora, la mejor organizadora de comidas; ¡ánimo!), a los compañeros que ya se han ido, Ignacio, Jose, David, Arancha y Víctor F., y a los que acaban de llegar, Marta y Alberto. Gracias a todos por vuestra maravillosa compañía, ayuda, comidas y cafés, y por todos los buenos momentos que hemos pasado juntos. También me gustaría dar las gracias al resto de miembros del departamento: Fausto, Amalia, Amparo, Luis, Gerardo, Gonzalo y Jaime, y a todo el personal del centro Torres Quevedo. Me gustaría expresar, si fuera posible, mi más cariñoso agradecimiento a mi compañero y amigo Agus. No existen palabras ni idiomas en este mundo para agradecerte todo lo que has hecho por mí, pero lo intentaré con algunas: *no me, puentes, . . . ya sabes*.

Durante mis años de doctoranda tuve la oportunidad de colaborar con otros grupos de investigación para profundizar en otras áreas de la criptografía cuántica. Quisiera agradecer especialmente al profesor Gerald Buller de la universidad Heriot-Watt (HWU) de Edimburgo y al profesor Harald Weinfurter de la Ludwig-Maximilian-Universität (LMU) de Múnich, su inestimable hospitalidad

---

y colaboración. También me gustaría dar las gracias a Patrick Clarke y Robert Collins de HWU, y a Sebastian Nauerth, Almut Tröller y Daniel Schlenk de LMU, por su amable bienvenida y trato cercano. Me gustaría agradecer especialmente a Patrick las horas tan divertidas en el laboratorio (y fuera de él); ¡teníamos que haber inventado la distribución cuántica de galletas!

No me puedo olvidar de mi grupo madrileño (Eli, Miguel, Etor, Germán, Dani y Álvaro); de mis queridísimas Soni, Sofi y Tana; de mi grupo de Las Brisas (Isa, Lorena, Mamen, Lola, Belén, Merche y Patri); y de Kuquen y Gema; muchas gracias, sé cuánto os alegráis por mí.

A mis amigos y familia, María José (mi amiga del alma), Rafa, Raquel y Antonio, gracias por animarme tanto, y también a mi nueva familia (Rita, Paco, Patri, Isabel, Alfonso, Jose Mari, Salva y Adriano) por vuestro cariño, apoyo y buenos momentos juntos.

Gracias a mi hermana Nuria por quererme, animarme y a la vez devolverme la cordura cuando he flaqueado, y a mi hermano Jorge por cuidarme siempre y por tu gran amor incondicional. Muchas gracias también a mis cuñados Víctor y Toñi, especialmente por haberme dado esos maravillosos, guapos, inteligentes y adorables sobrinos, Esther, Víctor y Emma, que son la alegría de mi vida.

Finalmente, esta tesis es un regalo para mi Miguel (¡feliz cumpleaños!, ¡prepárate para las uvas!). Miguel, haces que la vida sea tan fácil y maravillosa. . . , gracias por quererme tanto y tan bien. También es una muestra de amor hacia mis padres, Pepe y Fina, para expresarles mi agradecimiento por su cariño, buenos consejos y aliento, y por ser los mejores padres y el mejor ejemplo de esfuerzo y bondad que jamás hubiera podido tener.

## Acknowledgements

I would like to express my deepest gratitude to the director of this PhD thesis, Dr. Verónica Fernández Mármol, for guiding me through the fascinating world of quantum cryptography. I will always be very grateful for her mostly personal and friendly treatment, and also for her determination and great effort at leading the ‘quantum’ group. I would also like to thank the tutor of this thesis, Prof. José Manuel Calleja, for his invaluable support and patience.

I would like to express my sincere gratitude to my ‘quantum’ colleagues Natalia Denisenko and Diego Soto, who know firsthand the hard work to get the system operating. The long hours spent together in the laboratory and the fruitful discussions were a great experience that I really appreciate. Thanks also to my other colleagues: Juanca (for your tiramisu and your lovely treatment), Mari Carmen (your nice encouragement), Alfonso (your compliments in the corridor), Nacho (I want the divorce and I keep the division calculation), Jesús (a great photographer but a better friend). Thanks to my beloved ‘PhD colleagues’ Alex (lucky Alejandro, it was great and a lot of fun to share the desk with you; come on!) and Carmen (so sweet and the best organising meals; courage!), to the colleagues who have already left, Ignacio, Jose, David, Arancha, and Víctor F., and to those who have just arrived, Marta and Alberto. Thanks to you all for your cheerful company, help, lunch and coffee times, and really great time spent together. I would also like to acknowledge the other members of the department: Fausto, Amalia, Amparo, Luis, Gerardo, Gonzalo and Jaime and all the staff of the Torres Quevedo centre. I would like to express, if possible, my most sincere gratitude to my colleague and friend Agus. There are neither words nor languages in this world to thank you for all what you have done for me, but I will try some: *no me, puentes, . . . ya sabes*.

During the past years I had the opportunity to collaborate with other research groups to get insight into other techniques in the field of quantum cryptography. I would like to express my special gratitude to Prof. Gerald Buller from Heriot-Watt University (HWU) of Edinburgh and to Prof. Harald Weinfurter from the Ludwig-Maximilian-Universität (LMU) München for their inestimable collaboration and hospitality. I would also like to thank Patrick Clarke and Robert Collins from HWU, and Sebastian Nauerth, Almut Tröller

---

and Daniel Schlenk from LMU, for their friendly welcoming and close treatment. I would like to specially thank Patrick for the funny hours in the lab (and outside the lab); we should have invented quantum cookie distribution!

I would also like to thank my Madrilenian group (Eli, Miguel, Etor, Germán, Dani and Álvaro); my beloved Soni, Sofi and Tana; my Brisas group (Isa, Lorena, Mamen, Lola, Belén, Merche and Patri); and to Kuquen and Gema, I know you are really happy for me.

To my friends and family María José (my soul mate), Rafa, Raquel and Antonio, thank you for always cheering me up, and also to my new family (Rita, Paco, Patri, Isabel, Alfonso, Jose Mari, Salva and Adriano) for your love, support and great time spent together.

Thanks to my sister Nuria for loving and encouraging me and for keeping me with my feet on the ground, and to my brother Jorge for always taking care of me and for your immense unconditional love. I would also like to thank my brother and sister in law, Víctor and Toñi, especially for giving me those lovely, pretty, intelligent, adorable, nieces and nephew: Esther, Emma and Víctor, who are the joy of my life.

Finally, this thesis is a present for my Miguel (Happy birthday! Prepare yourself for the grapes!). Miguel, close to you life is so easy and wonderful. . . , thank you for loving me so much and so well. It is also a token of my love for my parents, Pepe and Fina, to express them my gratitude for their love, guidance and encouragement, and for being the best parents and the best example of sacrifice and goodness I could ever have.

# Contents

<b>Introducción</b>	<b>1</b>
Introducción y objetivos . . . . .	1
Contenido . . . . .	3
<b>Conclusiones y trabajo futuro</b>	<b>7</b>
Conclusiones . . . . .	7
Trabajo futuro . . . . .	12
<b>1 Introduction</b>	<b>15</b>
1.1 Introduction and objectives . . . . .	15
1.2 Outline . . . . .	17
<b>2 Quantum Key Distribution</b>	<b>19</b>
2.1 Brief introduction to Cryptography . . . . .	20
2.1.1 Symmetric ciphers. The problem of key distribution . . . .	25
2.1.2 Asymmetric ciphers . . . . .	27
2.1.3 Security of classical Cryptography. The threat of quantum computing . . . . .	28
2.1.4 The birth of Quantum Cryptography . . . . .	30
2.2 Quantum Key Distribution protocols . . . . .	30
2.2.1 Classification of QKD protocols . . . . .	31
2.2.2 The BB84 protocol . . . . .	32

2.2.3	The B92 protocol . . . . .	34
2.2.4	Error correction and privacy amplification . . . . .	36
2.3	Components in a QKD system . . . . .	38
2.3.1	Transmitter. Emission of single photons . . . . .	38
2.3.2	Channel: optical fibre or free space . . . . .	39
2.3.3	Receiver. Detection of single photons . . . . .	42
2.4	Security of QKD . . . . .	43
2.4.1	Quantum bit error rate . . . . .	43
2.4.2	Security foundations of QKD . . . . .	44
2.4.3	Attacks to QKD systems . . . . .	45
2.4.4	Device-Independent Quantum Cryptography . . . . .	54
2.5	Experimental free-space QKD systems . . . . .	55
<b>3</b>	<b>Design and characterisation of the transmitter</b>	<b>61</b>
3.1	Setup of the transmitter . . . . .	62
3.2	Generation of Alice's sequence . . . . .	64
3.3	Source of single photons . . . . .	64
3.3.1	Vertical-cavity surface-emitting lasers . . . . .	65
3.3.2	Wavelength choice . . . . .	66
3.3.3	Driver and circuit board interface . . . . .	67
3.3.4	Optimisation of the driving conditions of the VCSELs . . . . .	72
3.3.5	Spectral analysis . . . . .	75
3.4	Characterisation of the polarisation states . . . . .	78
3.5	Optical synchronisation . . . . .	82
3.6	Beams alignment . . . . .	83
3.7	Gimbal system . . . . .	86
3.8	Shielding the emitter from background radiation . . . . .	87
3.9	Conclusions . . . . .	88



<b>4</b>	<b>Free space as the quantum channel</b>	<b>91</b>
4.1	Factors affecting free-space QKD . . . . .	92
4.1.1	Line of sight requirement between Alice and Bob . . . . .	92
4.1.2	Sources of loss . . . . .	93
4.1.3	Atmospheric effects on beam propagation . . . . .	95
4.1.4	Weather conditions . . . . .	101
4.1.5	Background light . . . . .	102
4.2	Free-space optics used in the QKD system . . . . .	102
4.2.1	Design of the transmitter telescope and collimation of the output beam . . . . .	103
4.2.2	Receiver telescope . . . . .	105
4.2.3	Optical path: from the laser sources to the detectors . . .	106
4.2.4	Alignment of the transmitter and receiver telescopes . . .	111
4.3	Conclusions . . . . .	112
<b>5</b>	<b>Design and characterisation of the receiver</b>	<b>115</b>
5.1	Setup of the receiver . . . . .	116
5.2	Configuration of the optics module . . . . .	117
5.3	Single-photon detection . . . . .	118
5.3.1	Single-photon detectors operating at a wavelength of 850 nm . . . . .	121
5.3.2	Single-photon avalanche diodes . . . . .	123
5.3.3	PerkinElmer Single Photon Counting Module . . . . .	126
5.4	Time Interval Analyser . . . . .	127
5.5	Analysis and correction of the polarisation extinction ratio . . .	129
5.6	Receiver loss . . . . .	131
5.7	Detection of the synchronisation signal at the receiver . . . . .	134
5.8	Filtering and shielding from background light . . . . .	136
5.9	Conclusions . . . . .	139

<b>6</b>	<b>Experimental results for two optical links</b>	<b>141</b>
6.1	Setup and location of the QKD links . . . . .	142
6.2	The key exchange protocol . . . . .	144
6.2.1	Calculation of the QBER . . . . .	145
6.2.2	Estimation of the secret key rate . . . . .	145
6.3	Experimental results . . . . .	147
6.3.1	Optimum clock frequency . . . . .	148
6.3.2	Optimum mean photon number per pulse . . . . .	151
6.3.3	Influence of background radiation . . . . .	152
6.3.4	Stability of the system . . . . .	153
6.3.5	System robustness to misalignment . . . . .	156
6.4	Characterisation of the contributions to the QBER . . . . .	157
6.5	Maximum achievable distance and turbulence . . . . .	161
6.6	Conclusions . . . . .	162
<b>7</b>	<b>Conclusions and future work</b>	<b>165</b>
7.1	Conclusions . . . . .	165
7.2	Future work . . . . .	170
	<b>References</b>	<b>173</b>
	<b>Glossary</b>	<b>205</b>
	<b>Alphabetical index</b>	<b>207</b>

# List of figures

2.1	Skytale was the first cryptographic device implementing permutations. . . . .	21
2.2	Alberti's disc was the first cryptographic device implementing substitutions. . . . .	22
2.3	The Vigenère polyalphabetic cipher allowed the use of 26 different cipher alphabets for fast encryption/decryption. . .	23
2.4	Cryptogram using the Vigenère polyalphabetic cipher with the key "MJGMCDT". . . . .	24
2.5	Scheme of a symmetric cryptographic transmission. . . . .	26
2.6	Scheme of an asymmetric cryptographic communication. . . . .	28
2.7	Example of a cryptographic system based on quantum key distribution. . . . .	31
2.8	Schematic view of the BB84 protocol. . . . .	32
2.9	Example of B92 photon polarisation and bit encoding. . . . .	35
2.10	Experimental scheme at Bob for the detection of the two non-orthogonal polarisation states '0' and '1'. . . . .	36
2.11	Typical profile of the Rate versus Distance curve for a fibre-based QKD link . . . . .	40
2.12	Efficiency curves showing the mismatch between the states received by Bob's detectors. . . . .	51
3.1	Diagram of the transmitter: Alice. . . . .	62
3.2	Picture of Alice module. . . . .	63

3.3	Schematic gain structure of a VCSEL. . . . .	66
3.4	Input-output characteristics of the laser. . . . .	67
3.5	Photographs of the front (left) and back (right) of the MAX3795 driving board. . . . .	68
3.6	Extinction ratio of the optical output of VCSEL1 vs. $R_{MODSET}$ . . . . .	69
3.7	Extinction ratio of VCSEL1 against the bias current for a maximum modulation current at 1 GHz clock frequency. . . . .	70
3.8	Jitter of the electrical input of the MAX3795 driver and the optical output of the VCSEL0 against clock frequency. . . . .	71
3.9	Eye diagrams of the electrical input of the laser driver and the optical output emitted by VCSEL0 at three clock frequencies. . . . .	72
3.10	Schematic of the experimental setup for the optimisation of the driving conditions of the VCSELs. . . . .	73
3.11	Quantum bit error rate against the bias current of VCSEL0 at three particular values of the modulation current and 1 GHz clock frequency. . . . .	74
3.12	Quantum bit error rate against $R_{MODSET}$ for both VCSEL0 and VCSEL1 at the optimum bias current of 2 mA and 1 GHz clock frequency. . . . .	75
3.13	Central emission wavelength of VCSEL0 against the bias current (left) and against the clock frequency (right). . . . .	76
3.14	Emission spectra of VCSEL0 at three different bias currents (left) and at two modulation currents (right). . . . .	77
3.15	Spectra of VCSEL0 in two different instants (left) and zoom of the spectra showing a shift of 14 pm (right). . . . .	77
3.16	PER of linearly polarised light incident on the cube beamsplitter and PER of the light after being transmitted through, against the angle of incidence. . . . .	79
3.17	PER of linearly polarised light incident on the first mirror in Alice, reflected by the first mirror, and after the second mirror, as a function of the angle of incidence. . . . .	80

3.18	PER of the light exiting Alice (from the transmission channel at the beamsplitter) against the angle of polarisation set in $P_1$ .	81
3.19	Polarisation extinction ratio of the quantum states at Alice's output against the incident angle of polarisation.	81
3.20	Schematic of the synchronisation process.	82
3.21	Method for the alignment of the three beams exiting Alice.	85
3.22	Method for making the three beams from Alice coincident by using a curved mirror and a CCD camera.	85
3.23	Pictures taken by the CCD camera of the '1' and '0' spots, showing that they were coincident.	86
3.24	AutoCAD design (left) and picture (right) of the gimbal system for the transmitter.	87
3.25	Alice mounted on a robust tripod.	88
3.26	Pictures of the transmitter with the antireflective tube and with the shielding fabric and card.	88
4.1	Rayleigh scattering cross section as a function of wavelength.	97
4.2	Atmospheric transmittance as a function of wavelength under urban aerosol conditions and a visibility of 5 km (data simulated with MODTRAN 4.0).	98
4.3	Atmospheric transmittance versus wavelength considering two types of aerosol scenarios: rural extinction with a visibility of 23 km and urban extinction with a visibility of 5 km (data simulated using MODTRAN 4.0).	99
4.4	Schematic of the free-space optics used for the QKD link.	102
4.5	Beam radius $\omega$ against the propagation distance $z$ for several values of the beam waist at the transmitter aperture $w_0$ .	104
4.6	Collimation method of Alice's output beam using the receiver telescope and a CCD camera.	105
4.7	Diagram of Meade Schmidt-Cassegrain 8 inch LX200GPS.	106
4.8	The Schmidt-Cassegrain telescope with Bob's optics attached to it.	107

4.9	Setup of the free-space optics. . . . .	107
4.10	Geometry of the imaging of a Gaussian beam by a lens, shown for the case of a positive lens and real object and image waists. .	108
4.11	Waist diameter of the beam after lens L4 (left) and its divergence (right) against the distance between L4 and $d_{f3}$ . . . .	111
4.12	Schematic of the method used to establish parallelism between the alignment beam ( $\lambda \sim 650$ nm) and the beams carrying information at $\lambda \sim 850$ nm and $\lambda \sim 1550$ nm. . . . .	112
5.1	Diagram of the receiver. . . . .	116
5.2	Picture (left) and diagram (right) of the receiver's optics. . . .	117
5.3	Normalised instrument responses for the indicated detectors. . .	122
5.4	Schematic of a <i>reach-through</i> avalanche photodiode structure. .	125
5.5	Typical trace of the photocurrent of an APD. . . . .	126
5.6	Polarisation degradation after the dichroic mirror at $\lambda \sim 850$ nm .	129
5.7	Effect of two consecutive quarter-wave plates on the polarisation of two non-orthogonal states. . . . .	130
5.8	PER of the non-orthogonal polarisation states at the receiver in three cases: (a) without applying any polarisation-correcting measure, (b) improving the vertical state in ch1 by using a $\lambda/2$ plate, and (c) improving the diagonal state in ch0 by using two $\lambda/4$ plates. . . . .	132
5.9	Transmission curves of the Meade telescope. . . . .	133
5.10	Screen capture of the synchronisation signal measured at the output of the InGaAs photodetector. . . . .	135
5.11	Screen capture of the synchronisation signal measured at the output of the trans-impedance amplifier. . . . .	135
5.12	Transmittance of the interference filter and optical power emitted by VCSEL1 against the wavelength. . . . .	137
5.13	Picture of the receiver covered with the blackout fabric. . . . .	138

6.1	View from the transmitter's side to the receiver (left) and aerial view of the 30 meter link (right). . . . .	142
6.2	View from the transmitter's side to the receiver (left) and aerial view of the 300 meter link (right). . . . .	143
6.3	QBER, $R_{sifted}$ and $R_{net}$ against clock frequency for a 30 meter optical link. . . . .	148
6.4	Comparison between both optical links in terms of QBER, $R_{sifted}$ and $R_{net}$ as a function of the clock frequency. . . . .	150
6.5	QBER, $R_{sifted}$ and $R_{net}$ against the mean photon number per pulse $\mu$ for a 300 meter optical link. . . . .	151
6.6	QBER, background rate and $R_{net}$ measured the 22 <sup>nd</sup> of May 2012 for a 30 meter optical link at a clock frequency of 1 GHz. .	152
6.7	QBER, background rate and $R_{net}$ measured the 31 <sup>st</sup> of July 2012 for a 300 meter optical link at the optimum clock frequency (1.5 GHz). . . . .	153
6.8	QBER, $R_{sifted}$ , $R_{net}$ and background rate during a 24-hours experiment for a 30 meter optical link. . . . .	154
6.9	$R_{sifted}$ and temperature data from Madrid–Barajas meteorological station along a 24-hours experiment. . . . .	155
6.10	QBER, $R_{sifted}$ , $R_{net}$ and background rate during a 24-hours experiment for a 300 meter optical link. . . . .	156
6.11	QBER and $R_{net}$ against an intentionally-caused misalignment at the emitter. . . . .	157
6.12	Comparison of computed QBER with estimated QBER at different clock frequencies for the 30 meter optical link. . . . .	160
6.13	Comparison of computed QBER with estimated QBER and the QBER component due to background radiation measured the 22 <sup>nd</sup> of May 2012 for a 30 meter optical link operating at a clock frequency of 1 GHz. . . . .	160





# List of tables

5.1	Characteristic parameters of specific detectors when used at a wavelength of 850 nm. . . . .	121
5.2	Comparison of several relevant features for four PerkinElmer SPCMs. . . . .	127
5.3	Total loss of the receiver and optical loss of each optical component. . . . .	131
6.1	Quantum bit error rate due to intersymbol interference at different clock frequencies. . . . .	159
6.2	Maximum transmission distance the QKD system can withstand considering several regimes of turbulence. . . . .	162



# Introducción

## Introducción y objetivos

La transmisión cuántica de clave (QKD del inglés *Quantum Key Distribution*) [[Bennett et al., 1984](#)], más conocida como criptografía cuántica, se ha convertido en un nuevo paradigma en la protección de datos. La seguridad de las comunicaciones de datos cifradas con claves intercambiadas con QKD recae en las leyes de la Mecánica Cuántica, en lugar de en una capacidad computacional limitada asumida para un posible atacante. QKD permite que dos partes compartan una clave criptográfica teniendo al Principio de Incertidumbre de Heisenberg y al teorema de No Cloning [[Wootters et al., 1982](#)] como principales aliados. La novedad de esta estrategia es que los usuarios legítimos pueden detectar la presencia de un intruso en el canal y por tanto certificar la seguridad de la transmisión.

Los principales trabajos sobre QKD en espacio libre se centraron inicialmente en conseguir largas distancias de transmisión con el objetivo de probar la viabilidad de las comunicaciones QKD vía satélite [[Schmitt-Manderbach et al., 2007](#)]. Sin embargo a cortas distancias (rango interurbano) los enlaces de QKD en espacio libre también encuentran una aplicación importante, ya que pueden en parte aliviar el problema del ‘cuello de botella’ que afecta a la conectividad de las redes metropolitanas. Además, en general, la óptica en espacio libre (FSO del inglés *Free Space Optics*) tiene una ventaja considerable sobre la fibra óptica que radica en su flexibilidad de instalación y portabilidad. A diferencia de la fibra óptica, que se convierte en un coste irrecuperable

cuando el cliente abandona su ubicación, los enlaces FSO pueden ser trasladados como se requiera. QKD aplicada a enlaces aéreos cortos en zonas urbanas se convierte así en una alternativa interesante a la criptografía de clave pública actual, la cual está amenazada por la llegada del ordenador cuántico. En este contexto la QKD está orientada principalmente para su uso en instituciones de carácter financiero, gubernamental o militar situadas en una misma ciudad. Sin embargo, para que la QKD pueda ser una alternativa realista necesita implementarse a alta velocidad de forma que las claves secretas sean generadas a altas velocidades y puedan ser utilizadas en tándem con el cifrado *one-time pad* [Vernam, 1926], que es el único cifrado ‘irrompible’ que se ha propuesto hasta la fecha.

Por lo tanto, los principales objetivos de esta tesis han sido el diseño y la implementación de un sistema de QKD a alta velocidad en espacio libre. Para conseguir QKD a alta velocidad hay que tener en cuenta diversas cuestiones. La selección de la longitud de onda y los detectores es crítica, así como el diseño del transmisor y del receptor o el método de sincronizado. En comunicaciones ópticas en espacio libre se utilizan normalmente dos ventanas espectrales con baja absorción en las regiones de infrarrojo cercano, concretamente en las longitudes de onda de 850 nm y 1550 nm. Aunque la segunda tiene asociada una mayor transmisión y se ve menos afectada por las turbulencias y el *backscattering*, la tecnología de detección de fotones también debe ser considerada. De hecho, aunque los detectores de fotones individuales de InGaAs han mejorado considerablemente su rendimiento mediante el incremento de su máxima frecuencia de operación (de MHz a GHz), todavía son superados por los diodos de avalancha de único fotón de Silicio (Si-SPADs) en parámetros críticos tales como cuentas oscuras, eficiencia de detección y probabilidad de *afterpulsing*. De la misma manera, los detectores de fotones individuales superconductores, aunque exhiben bajos *jitters* temporales y pocas cuentas oscuras a  $\lambda \sim 850$  nm [Clarke et al., 2011], presentan menores eficiencias que los Si-SPADs, además de tener que ser enfriados a temperaturas tan bajas como 3 K. Tras analizar los factores mencionados se optó por seleccionar una fuente de fotones a una longitud de onda de 850 nm y Si-SPADs como detectores de fotones individuales, por considerar esta combinación la opción más práctica para conseguir velocidades de GHz.

En general, para el diseño de un transmisor y un receptor capaces de operar a altas velocidades de transmisión de datos es necesario considerar varios factores clave: una fuente de fotones que permita velocidades de GHz y muy alta precisión temporal, un receptor capaz de procesar grandes cantidades de datos a alta velocidad, y un mecanismo de sincronización que no disminuya la velocidad del protocolo QKD. Además, abordando factores críticos tales como una alta linealidad de los estados cuánticos de polarización y una eficiente reducción de la radiación ambiental que se cuela en el sistema, se consiguen tasas de error bajas, y por lo tanto altas velocidades de transmisión de clave segura. A continuación se proporciona un breve resumen de los contenidos de cada capítulo de esta tesis.

## Contenido

Los contenidos de esta tesis se han organizado de la siguiente manera.

En el Capítulo 2 se introduce el concepto de QKD. En primer lugar se describen los principales logros conseguidos en el campo de la criptografía a lo largo de la historia. A continuación se presenta el contexto de la criptografía previo al nacimiento de la QKD, señalando las vulnerabilidades de los algoritmos de cifrado clásicos que se utilizan actualmente. La QKD se presenta entonces como una posible solución frente a estas vulnerabilidades. También se describen los protocolos más representativos que implementan QKD y los componentes necesarios en un sistema de QKD. Finalmente se resumen los principales ataques a la QKD y se presenta una revisión de los sistemas experimentales de QKD en espacio libre implementados hasta la fecha.

El Capítulo 3 está dedicado a la descripción del módulo transmisor, diseñado e implementado para el sistema de QKD que se describe en esta tesis. Se describen además varios experimentos realizados para caracterizar el comportamiento del transmisor en función de las corrientes de control de los láseres (bias y modulación), así como el comportamiento espectral de éstos. Asimismo se describe la caracterización de la linealidad de los estados de polarización que codifican la secuencia binaria enviada por Alice, el método de sincronización temporal y las técnicas usadas para aislar el emisor de la radiación ambiental,

entre otros. Este capítulo concluye con una descripción del equipo donde se montó el emisor.

El Capítulo 4 trata sobre el canal de transmisión. En él se resumen los diferentes procesos que afectan a la propagación de los fotones a través del espacio libre, tales como la absorción atmosférica, el *scattering* o la turbulencia. También se estudia el efecto de la radiación ambiental que puede colarse en el sistema de QKD incrementando el error. Finalmente se describe la óptica en espacio libre utilizada en emisor y receptor para aumentar la eficiencia de la detección de la señal óptica en Bob, lo que se traduce en una mejora de la velocidad de transmisión de clave.

El Capítulo 5 está dedicado a proporcionar una descripción detallada del módulo del receptor. En primer lugar se describe la configuración de esta unidad. Después se detallan los módulos utilizados para la detección de fotones individuales y para el procesamiento de los tiempos de llegada de éstos al receptor. También se presenta la caracterización y corrección llevadas a cabo en el receptor de los estados de polarización. Al final de este capítulo se describe la detección de la señal de sincronizado y las técnicas empleadas para el filtrado de la radiación ambiental.

En el Capítulo 6, se proporciona una descripción de los experimentos realizados para caracterizar el sistema de QKD completo y se presentan los resultados obtenidos para dos enlaces ópticos a diferentes distancias. También se describe el programa desarrollado para el cálculo del error de cada transmisión y para la corrección del desfase temporal entre las secuencias de emisor y receptor. Los experimentos llevados a cabo se diseñaron para determinar la frecuencia óptima del sistema así como el número medio de fotones por pulso para el que la tasa de transmisión de clave segura fuera máxima. También se caracterizó la influencia de la radiación ambiental, la estabilidad del sistema y la robustez del mismo frente a perturbaciones externas que pudieran afectar el alineamiento entre ambas estaciones. El capítulo finaliza con una estimación de la máxima distancia a la que el sistema puede operar, para varios regímenes de turbulencia.

Finalmente el Capítulo 7 resume las conclusiones de los capítulos anteriores y proporciona ideas sobre posibles modificaciones a realizar en el sistema

de QKD presentado en esta tesis con el objetivo de mejorar su seguridad, velocidad de transmisión de clave segura y distancia de transmisión.

## Referencias

1. C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing”, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179 (1984).
2. W. K. Wootters, and W. H. Zurek, “A single quantum cannot be cloned”, Nature, 299, Page 802-803 (1982).
3. T. Schmitt-Manderbach et al., “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km”, Phys. Rev. Lett. 98, 010504 (2007).
4. G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications”, Journal of the American Institute of Electrical Engineers, 45, Page 109-115 (1926).
5. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Gigahertz quantum key distribution with InGaAs avalanche photodiodes”, Appl. Phys. Lett. 92, 201104 (2008).
6. P. J. Clarke, R. J. Collins, P. A. Hiskett, M. J. García-Martínez, N. J. Krichel, A. McCarthy, M. G. Tanner, J. A. O’Connor, C. M. Natarajan, S. Miki, M. Sasaki, Z. Wang, M. Fujiwara, I. Rech, M. Ghioni, A. Gulinatti, R. H. Hadfield, P. D. Townsend, and G. S. Buller, “Analysis of detector performance in a gigahertz clock rate quantum key distribution system”, New J. Phys. 13, 075008 (2011).





# Conclusiones y trabajo futuro

Este capítulo ofrece un resumen de los resultados y conclusiones obtenidos de la implementación y caracterización del sistema de QKD presentado en esta tesis. También se recogen las aportaciones del presente trabajo al campo de la criptografía cuántica. Por último, se proponen posibles actualizaciones y modificaciones del sistema de QKD descrito, que podrían aumentar su tasa de clave segura así como la distancia de transmisión.

## Conclusiones

La presente tesis aporta una descripción detallada de un sistema de transmisión cuántica de clave en espacio libre, que implementa el protocolo B92 a altas velocidades de transmisión en un entorno urbano. Las conclusiones más relevantes extraídas del diseño y caracterización del sistema así como del estudio del área se resumen a continuación.

1. Teóricamente, QKD en tándem con el cifrado de Vernam ofrece el nivel más alto de seguridad de entre todas las técnicas desarrolladas hasta la fecha, así como perspectivas de seguridad en un futuro en el que los ordenadores cuánticos formen parte de nuestra vida diaria. Sin embargo, para ser realmente competitiva todavía se han de solventar diversos aspectos como una mayor robustez ante los ataques por canal lateral, mayores distancias de transmisión y tasas más altas de clave segura.

2. En implementaciones experimentales de sistemas de QKD un espía puede obtener información de las ‘huellas’ que dejan los dispositivos físicos utilizados. Un sistema de QKD debe ser por ello cuidadosamente diseñado de forma que todas las posibles vulnerabilidades o *fisuras* experimentales se tengan en cuenta y se determine la fuga de información que dichas fisuras pudieran producir, para así establecer las pruebas de seguridad apropiadas. Sin embargo, el debate sobre las estrategias adecuadas para conseguir que la QKD sea segura en presencia de estas fisuras es intenso y muy abierto [Yuan et al., 2011b]. Todavía no se ha encontrado una solución satisfactoria, lo que pone de manifiesto la necesidad de una prueba de seguridad más general que incorpore el uso de dispositivos imperfectos. Acín *et al.* propusieron una estrategia denominada criptografía cuántica independiente de los dispositivos [Acín et al., 2007], aunque su realización experimental supone todavía un gran reto tecnológico. Después de casi tres décadas de su nacimiento, la criptografía cuántica ha alcanzado su madurez y se enfrenta probablemente a su reto más difícil: seguridad incondicional en un mundo ‘imperfecto’.
3. Para conseguir altas velocidades de transmisión el emisor del sistema de QKD descrito utiliza dos VCSELs con gran ancho de banda modulados por un generador de patrón de pulsos que opera a frecuencias de GHz. El régimen de emisión de fotones individuales se consigue atenuando los diodos láser a un número medio de fotones por pulso de aproximadamente 0.1. Los VCSELs se optimizaron en función de sus niveles de corrientes de control (modulación y *bias*) para minimizar su contribución a la tasa de error causada por interferencia entre símbolos. La corriente de *bias* óptima es de 2 mA y la de modulación en torno a 6 mA, con una contribución al QBER de menos del 0.5% para una frecuencia reloj de 1 GHz. El análisis de los espectros de los láseres reveló que estos apenas cambian con la corriente de modulación, frecuencia reloj o tiempo de funcionamiento. El desplazamiento de los espectros con la corriente de *bias* era de unos 0.15 nm/mA para valores altos de corrientes, y de aproximadamente la mitad para corrientes mínimas de *bias*.
4. El receptor del sistema de QKD analiza la polarización de los fotones que le llegan según el protocolo B92. Como detectores del sistema se

seleccionaron dos SPADs, debido a su alta eficiencia, bajo ruido, facilidad de uso y disponibilidad comercial. Se caracterizaron cuatro Si-SPADs en términos de su eficiencia de detección, tasa de cuentas oscuras y contribución al QBER. Los dos SPADs con mejor comportamiento presentaban eficiencias de detección de 29% y 35%, y tasas de cuentas oscuras de 170 y 250 cuentas/s, respectivamente. La tarjeta utilizada para medir y almacenar los tiempos de llegada de los fotones detectados consiste en un Analizador de Intervalos de Tiempo GT658PCI de GuideTech. La interfaz de usuario de LabVIEW suministrada con la tarjeta se modificó para monitorizar la tasa de cuentas en cada canal de entrada a la tarjeta y para proporcionar las listas de tiempos de llegada de los fotones a cada canal del receptor. Cada estado de polarización es detectado en un canal diferente.

5. Con el fin de aumentar la eficiencia en la recepción de los fotones emitidos por Alice se utilizó un telescopio en cada extremo del sistema de QKD. En Bob, además del telescopio Schmidt-Cassegrain, se montaron dos lentes con una distancia focal de 30 mm para mejorar el acoplamiento del haz en las fibras.
6. Para alinear ambas estaciones, Alice se montó en un sistema gimbal de alta precisión con dos motores rotatorios que proporcionaban los movimientos en azimuth y elevación necesarios para el correcto apuntamiento de Alice a Bob. El módulo óptico del receptor se acopló directamente al telescopio Schmidt-Cassegrain, cuyos motores facilitaron el alineamiento con el transmisor. A su vez, un láser visible a una longitud de onda de 650 nm emitía un haz paralelo a los haces de datos y de sincronización para facilitar el alineamiento burdo.
7. Los estados no ortogonales de polarización que cifran la información binaria son transmitidos en espacio libre desde Alice hacia Bob. La atmósfera constituye un excelente canal de transmisión debido a la ausencia de birrefringencia, lo que permite preservar los estados de polarización de los fotones. Además, en el entorno de  $\lambda \sim 850$  nm hay una ventana de baja absorción en la que existen detectores de fotones individuales eficientes. Sin embargo, factores como la atenuación atmosférica, las

condiciones climáticas y la turbulencia, limitan la máxima distancia de transmisión alcanzable. Las medidas realizadas en esta tesis se hicieron para enlaces ópticos en condiciones de partículas de aerosoles urbanos, y su atenuación se calculó con MODTRAN para una visibilidad de 5 km, resultando ser de unos 2 dB/km. Además, se hicieron cálculos para estimar la pérdida geométrica del haz en el receptor considerando diferentes regímenes de turbulencia. Las simulaciones revelaron que para un régimen de turbulencia intermedio ( $C_n^2 \approx 10^{-15}$ ) el sistema podría operar potencialmente hasta una distancia de 4.4 km.

8. Los sistemas de QKD en espacio libre también se ven afectados por la radiación solar ambiental así como por otras fuentes de luz ambiental que se acoplan en el sistema aumentando el error. Se implementaron técnicas de filtrado espacial y espectral, y además Alice y Bob fueron aislados mediante un tejido opaco y un tubo largo antireflectante colocado alrededor de la lente principal del telescopio de Alice. El filtro interferencial de 1 nm de FWHM redujo la radiación ambiental unos 30 dB, y el filtrado espacial llevado a cabo por las fibras ópticas con un núcleo de  $62.5 \mu\text{m}$  de diámetro proporcionó un campo de visión restringido al receptor. Estas técnicas de filtrado y aislamiento hicieron posible el funcionamiento diurno del sistema con altas velocidades de transmisión.
9. La relación de extinción de polarización para los dos estados cuánticos no ortogonales a  $\lambda \sim 850 \text{ nm}$  se caracterizó a lo largo de todo el sistema de QKD. En general, la absorción inherente a los materiales de ciertos componentes ópticos degradaba la linealidad de los estados de polarización, siendo particularmente significativa para el estado diagonal. Para contrarrestar dicho efecto se utilizaron una lámina de cuarto de onda en Alice y dos láminas de cuarto de onda más una lámina de media onda en Bob, con lo que se consiguieron relaciones de extinción de polarización que contribuyeron con menos de 0.25% al QBER total.
10. La sincronización óptica entre emisor y receptor se llevó a cabo mediante la emisión por parte de Alice de pulsos periódicos intensos a una longitud de onda de 1550 nm (diferente a la de los datos) y con una tasa de repetición de 10 MHz. La señal de sincronización electrónica para la

modulación del VCSEL de sincronizado se obtuvo de la salida de trigger del generador de patrón de pulsos del transmisor. En Bob se usó un fotodetector de InGaAs para su detección, y su nivel de voltaje fue mejorado mediante un amplificador de transimpedancia con el fin de obtener el voltaje requerido a la entrada de la señal de reloj externa de la tarjeta que mide los tiempos de llegada de los fotones.

11. La eficiencia de transmisión del canal (0.87 para un enlace de 300 m), la eficiencia total de la óptica del receptor (0.14), la eficiencia de detección de los SPADs (0.32), y la eficiencia del protocolo B92 (0.25) dieron como resultado una eficiencia total entorno a 0.01 para un enlace óptico de 300 m.
12. El sistema de QKD en espacio libre fue caracterizado para dos enlaces ópticos de diferente distancia, 30 m y 300 m, en un entorno urbano. La tasa de clave secreta fue calculada a partir de las medidas del QBER y de la tasa de la secuencia sifted, asumiendo el peor de los escenarios posibles en el que se estuvieran llevando a cabo dos ataques simultáneos: el ataque USD y el ataque PNS. Los siguientes resultados fueron obtenidos a partir de la caracterización del sistema:
  - La frecuencia reloj óptima para el funcionamiento del sistema, es decir, la que proporciona la tasa más alta de clave secreta, es 1.5 GHz. La frecuencia máxima a la que el sistema puede operar es 2.75 GHz, con un QBER por debajo del 8% en condiciones nocturnas.
  - El número medio de fotones por pulso óptimo es  $\mu \sim 0.1$ , con el que se consigue un compromiso óptimo entre seguridad y tasa de transmisión de la secuencia sifted.
  - El funcionamiento diurno del sistema ha sido demostrado en condiciones de radiación solar muy elevada, alcanzando tasas promedio de clave secreta de 0.7 Mbps para un enlace de 30 m y de 0.5 Mbps para 300 m.
  - En condiciones nocturnas se alcanzaron tasas de clave secreta de hasta 1 Mbps para el enlace de 300 m. Esta tasa de clave secreta es un orden de magnitud mayor que las alcanzadas previamente por otros sistemas en condiciones comparables.

- Se ha demostrado que el sistema es muy estable ya que, para el enlace de 300 m y después de un período de 24 horas con el sistema funcionando sin intervención alguna sobre él, las tasas que se obtuvieron de secuencia sifted y de clave secreta fueron el 87% y el 80%, respectivamente, con relación a sus valores al inicio del experimento.
- La robustez del sistema frente a posibles desalineaciones demostró que, sólo tras una reducción del 90% en la tasa de la secuencia sifted, se alcanzaban valores de QBER superiores al 6%. Esta tendencia indica que el sistema podría estar potencialmente alineado a 300 m durante 4 o 5 días sin intervención externa.

## Trabajo futuro

Como se ha mencionado en la primera conclusión, hay determinados aspectos de la QKD como su seguridad incondicional, la transmisión a grandes distancias o conseguir mayores tasas de clave segura, en los que se debería realizar un gran esfuerzo con el fin de conseguir que las implementaciones reales de sistemas de QKD sean verdaderamente competitivas.

En lo que respecta a la seguridad, el plan de investigación inmediato incluye mejorar el sistema de QKD discutido en esta tesis para implementar un protocolo más seguro frente a posibles atacantes, el protocolo BB84 con *decoy states*. Esto hará que el sistema sea invulnerable frente a los ataques PNS y USD, y aumentará la tasa de clave segura al menos un orden de magnitud. Para ello serán necesarios más componentes ópticos y mecánicos con el fin de incluir en el montaje los estados de polarización adicionales, así como dos VCSELs más en Alice, dos detectores más en Bob, y moduladores de intensidad para generar las diferentes intensidades de los decoy states.

Para hacer que el sistema sea más robusto frente a posibles ataques es esencial garantizar que los espectros de los láseres sean totalmente indistinguibles, de modo que no se suministre ninguna información extra al intruso. En el sistema actual los VCSELs son estables en potencia, puesto que los drivers de los láseres tienen un control automático de potencia que mantiene la potencia

óptica promedio de salida del láser estable ante posibles cambios de temperatura y de las propiedades del láser. Este control puede variar ligeramente la corriente bias del láser, lo que podría desplazar su espectro de emisión. Para asegurar una longitud de onda de emisión estable se prevé controlar la temperatura de los láseres. Esto permitiría sintonizar de manera precisa la longitud de onda de emisión de los VCSELs deseada, de forma que fuera idéntica para ambos láseres. Además, puesto que ambos VCSELs son multimodo, el control por temperatura permitiría usar un filtro paso-banda estrecho que asegurara la propagación de un único modo espectral.

En cuanto a la velocidad de transmisión de clave secreta, ésta podría mejorarse reduciendo el QBER del sistema. De día, la mayor contribución al QBER es la radiación ambiental. Para reducirla se ha diseñado una nueva configuración de Alice en la que los espejos son innecesarios. La implementación de la nueva configuración de Alice requerirá recolocar la óptica, lo cual implica modificar el conjunto de lentes del telescopio de salida y la placa óptica.

La radiación ambiental se podría reducir también usando un filtrado espacial más estrecho, por ejemplo con fibras ópticas de menor diámetro. Sin embargo, esto reduciría también el ángulo de aceptación del receptor, haciendo al sistema más vulnerable frente a turbulencias. Por lo tanto, otra optimización del sistema consiste en implementar técnicas automáticas de apuntamiento y seguimiento rápidos —actualmente en desarrollo— que permitan un funcionamiento continuo en condiciones de turbulencia en la atmósfera. Esto permitiría también aumentar la distancia del enlace óptico del sistema.

Por último, el sistema está siendo mejorado para la implementación de los procesos de corrección de errores y amplificación por privacidad en tiempo real, con el objetivo de generar la clave secreta final compartida por Alice y Bob.





# Chapter 1

## Introduction

### 1.1 Introduction and objectives

Quantum key distribution (QKD) [[Bennett et al., 1984](#)] —more generally known as quantum cryptography— has become a new paradigm in data protection. The laws of Quantum Mechanics, rather than assumed computational limitations, are now responsible for ensuring data communications. QKD allows two parties to share a cryptographic key, having Heisenberg’s uncertainty principle and No Cloning theorem [[Wootters et al., 1982](#)] as their principal allies. The novelty of this scheme is that the ‘quantumness’ of this properties allows the legitimate users to detect the presence of an eavesdropper in the channel and thus certify the security of the transmission.

Free-space QKD was primarily aimed towards satellite communications, and the main efforts have concentrated in achieving long distances to proof its feasibility [[Schmitt-Manderbach et al., 2007](#)]. However, short-distance (intra-city range) free-space QKD links are also of considerable importance, since they can partly alleviate the existing ‘connectivity bottleneck’ in metropolitan networks. Furthermore, free-space optics (FSO) in general, has a considerable advantage over optical fibre, namely their flexibility of installation and portability. Unlike optical fibre, which becomes an irrecoverable cost when the

customer leaves, FSO links can be moved to different locations as required. QKD applied to short free-space links in urban areas is an interesting alternative to current public-key cryptography, which is threatened by a quantum computer attack. In this context, QKD is aimed principally to financial, government and military institutions located within the same city. However, for QKD to be a realistic alternative, it needs to be implemented at high speed, so that secure keys can be generated at high rates to be used in tandem with the one-time pad [Vernam, 1926], the only unbreakable cipher proposed so far.

Therefore, the prime objectives of this thesis were the design and implementation of a high-speed QKD system in free space. Quantum key exchange at high rates can be achieved through several approaches. The choice of wavelength and detectors is critical as well as other considerations such as the design of the transmitter and receiver and the synchronisation method. Two low-absorption atmospheric spectral windows in the near-infrared regions of  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm are usually used in free-space optical communications. Although the latter wavelength has an associated higher transmission and it is slightly less affected by turbulence effects and backscattering, detection technology must also be considered. Indeed, while InGaAs single-photon detectors have greatly improved their performance in terms of the maximum repetition rate they can operate at (from MHz to GHz) [Yuan et al., 2008], they are still outperformed by commercially-available Si single-photon avalanche detectors (Si-SPADs) in critical parameters such as dark-count rate, detection efficiency and afterpulsing probability. Likewise, superconducting single-photon detectors, although exhibiting low timing jitters and low dark-count rates at  $\lambda \sim 850$  nm [Clarke et al., 2011], still show lower detection efficiencies than Si-SPADs, and must be cooled down to temperatures as low as 3 K. After analysing the mentioned issues, a source of photons of wavelength 850 nm in conjunction with Si-SPADs as the single-photon detectors was chosen as the most efficient and practical solution to achieve GHz clock rates.

In general, the design of a transmitter and a receiver capable of operating at high bit rates needs to take into consideration several key factors: an emitter allowing GHz clock rates with very high temporal precision, a receiver able to process large amounts of data without delaying the protocol speed, and a synchronisation mechanism that does not slow down the whole communication

transfer. Moreover ensuring the most critical factors are addressed, such as a high linearity of the polarisation quantum states and an efficient reduction in the background radiation, permits low error rates and hence high secure key rates. In the following a brief outline describing the contents of each chapter in this thesis is given.

## 1.2 Outline

The contents of this thesis are arranged as follows.

In chapter 2 the concept of QKD is introduced. Firstly, the main achievements through history in the field of cryptography are described. Then an overview of the context of cryptography previous to the birth of QKD is given, highlighting the vulnerabilities of the classical ciphers that are used to encrypt nowadays communications. Quantum key distribution is then presented as a possible solution to such vulnerabilities. The most representative protocols that implement QKD and the components involved in a QKD system are also discussed. Finally, the most relevant eavesdropping attacks against QKD are described, and a review of free-space experimental QKD systems is provided.

Chapter 3 is devoted to describe the configuration of the transmitter module, designed and implemented for the QKD system presented in this dissertation. Then, several experiments carried out to characterise and optimise the performance of the transmitter in terms of the driving conditions and spectral behaviour of the lasers, the linearity of the polarisation states encoding the binary sequence sent by Alice, the timing synchronisation technique or the shielding from solar radiation, are described among others. This chapter concludes with a description of the equipment where the transmitter is mounted on.

Chapter 4 discuss the transmission channel, outlining the different processes that may affect the propagation of photons through free space such as atmospheric absorption, scattering or turbulence. Also the effect of background radiation that may couple into the QKD system and increase the error rate is studied. Finally, the free-space optics used in both transmitter and receiver to enhance the efficiency of the channel and therefore the transmission rates is described.

Chapter 5 is intended to provide a detailed description of the implemented receiver module of the QKD system. The configuration of this unit is firstly discussed. Then, the modules used for the detection of single photons and the recording of their arrival times at the receiver are described. Also the characterisation and improvement of the detected polarisation states regarding their linearity are presented. At the end of this chapter, the detection of the synchronisation signal and the background filtering techniques are discussed.

In chapter 6 a description of the tests performed to characterise the entire QKD system and the experimental results obtained for two optical links of different distance are provided. Also the program developed to compute the error rate and to correct for the temporal shift between the transmitter's and receiver's sequences is explained. The experiments allowed establishing the optimum clock frequency and the optimum mean photon number per pulse for which the highest secret key transmission rate is achieved. The influence of background radiation, the system's stability and the robustness to external perturbations that might affect the alignment between both stations is also analysed. The chapter ends with an estimation of the maximum distance the system could operate at regarding several turbulence regimes.

Finally, chapter 7 summarises the conclusions of previous chapters and provides some clues about possible modifications that could be applied to the QKD system presented in this thesis to enhance its security, secret key rate and transmission distance.

## Chapter 2

# Quantum Key Distribution

Quantum Key Distribution (QKD) allows a theoretically secure key distribution over an untrusted channel, which is guaranteed by the laws of Quantum Mechanics. In this chapter a historical overview of the principles of Cryptography is first presented, briefly describing the main characteristics of symmetric and asymmetric ciphers. Then the threat that the birth of a quantum computer may pose to the security of these classical ciphers is remarked, and the concept of quantum cryptography as an alternative method to ensure communications is introduced. A brief description of the protocols most frequently used for its implementation and an overview of the main components of a QKD system are also described. The foundations of QKD security are then discussed, and the most relevant eavesdropping attacks against QKD systems are summarised. The chapter concludes with a section devoted to review up to date representative QKD experimental systems operating in free space.

## 2.1 Brief introduction to Cryptography

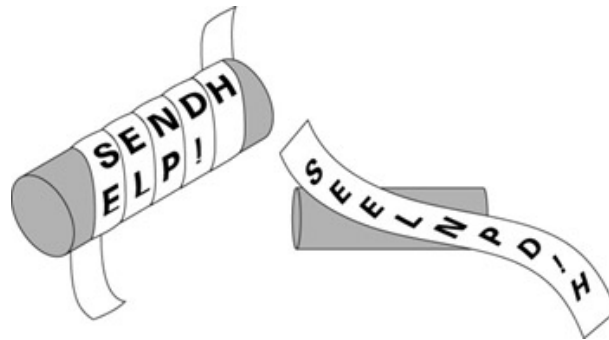
Throughout history, the old art of communicating secrets has constantly played an essential role in many contexts: political, economical, social, etc., with the military being of especial relevance. Nowadays the fast development and wide use of computers have dramatically increased the possibilities of cryptography, which has become an unnoticeable part of everybody's life whenever sensitive data like credit card information is sent through communication networks.

Cryptography is a science that studies the methods to securely transmit information between two parties, rendering the message unintelligible to any unauthorized third party. It is therefore the process of hiding information by modifying an ordinary message, known as *plaintext*, to obtain an apparently meaningless message or *ciphertext*, which is incomprehensible to anyone who ignores how it was generated. To achieve this, an algorithm (also called a *cryptosystem* or cipher) is used to combine a message with some additional information—known as the key—to generate a *cryptogram*. This process is called *encryption*. The reverse process to encryption, with the knowledge of the key, is called *decryption*. For a cryptosystem to be secure it should be impossible to decrypt the cryptogram without the key.

Cryptography is used nowadays not only to guarantee that solely the legitimate parties have access to the ciphered information (i.e., to ensure confidentiality), but also to cover further objectives such as authentication, digital signatures or non-repudiation. Cryptography is one of the two branches of the broader discipline of Cryptology, being the other one Cryptanalysis: the art of gaining unauthorized access to cryptosystems with the aim of obtaining information from ciphertexts without knowing the key or by acquiring the key itself, also known as *code breaking*.

From the beginnings of civilization humans have wished to communicate secretly. With the aim of concealing information the ancient Greeks wrote messages on wooden tablets, which later were covered with wax. The Spartans were the first to use a strictly speaking cryptographic system in warfare. They invented the *skytale*, a device which consisted of a wooden rod with a strip of papyrus or parchment wrapped around it. The sender would write a message on the strip from left to right along the length of the skytale (see Figure 2.1).

When the strip was unwound the message appeared as a list of meaningless letters. Then the message was conveyed to its destination and could only be readable by wrapping the strip around a rod with the same diameter as the original piece. The skytale is an example of a *transposition* cipher, where the letters of the plaintext are rearranged by a special permutation.

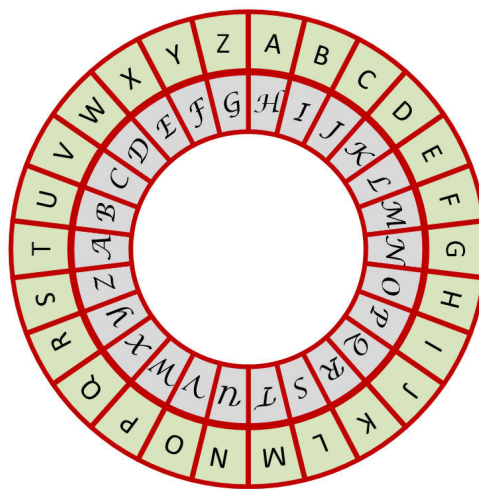


**Figure 2.1** – Skytale was the first cryptographic device implementing permutations.

The first *substitution* ciphers were used by the Romans. In a substitution cipher (also known as *Caesar cipher* since Julius Caesar made use of it to communicate with his generals) the characters of a plaintext are replaced by characters located a certain number of places further down the alphabet. A shift of three places was originally used, so that the letter A was replaced by D, the letter B by E, and so on. For example, the English word PLUG appears as MIRD after the substitution with this cipher. More generally, in substitution ciphers the letters of the plaintext are replaced by other letters, numbers or arbitrary symbols. Although easy to encrypt, ciphers based on one-to-one substitutions, also known as *monoalphabetic* ciphers, can be easily broken by *frequency analysis*, a cryptanalysis technique proposed in the ninth century by Al-Kindi that takes advantage of the known rate of recurrence of certain letters in a particular alphabet [Sergienko, 2006].

The above simple examples of ciphers already contained the two basic methods of encryption that are still employed by cryptographers today, namely transposition and substitution, techniques that can also be combined to produce more complex ciphers. Monoalphabetic ciphers were gradually replaced along the fifteenth and sixteenth centuries by more advanced techniques. In

the 1460s a device that simplified the use of Caesar ciphers was invented by Leon Battista Alberti (1404–1472). It consisted of two concentric discs with different characters (see Figure 2.2), used as plaintext and ciphertext alphabets respectively. After replacing a letter of a disc by its corresponding letter of the second disc, a rotation of the discs changed the relation between both alphabets. This allowed to easily modifying the cipher alphabet, so that a letter repeated a certain number of times in the plaintext did not produce a repeated character in the ciphertext.



**Figure 2.2** – Alberti’s disc was the first cryptographic device implementing substitutions.

Through his proposal of, by rotating the discs, varying the shift between both alphabets for each letter within the same message, Alberti would have discovered the so called *polyalphabetic* ciphers, which are basically a superposition of Caesar ciphers with different shifts that are established by the key. For instance, for the key 7–12–17, the first letter in the message is replaced by the character corresponding to a shift of 7 positions, the second of 12, the third of 17, the fourth again of 7, and so on repeating the shifts 7–12–17 until the whole message is ciphered. Using this key the message TABLE is transformed into the meaningless AMRSQ.

In 1586 Blaise de Vigenère, combining ideas from Alberti, Johannes Trithemius and Giovanni Porta, developed one of the most powerful and well known polyalphabetic ciphers, called after him the *Vigenère cipher*. It consists



in using the table shown in Figure 2.3, which contains 26 different cipher alphabets, instead of only one, to encrypt a message. The table is obtained by successively shifting each alphabet one position to the left. The top row in lower case contains the plaintext alphabet. Then each character of the key indicates the particular ciphertext alphabet that must be used to encrypt each character of the plaintext. If the key is not long enough, it is repeated and concatenated until it has the same length as the plaintext. Figure 2.4 shows an example of a plaintext encrypted with this scheme using the key “MJGMCDT”. With this key the first letter of the plaintext must be encrypted using alphabet “M” (row 12), the second with alphabet “J” (row 09), the seventh with alphabet “T” (row 19), the eighth with alphabet “M” again, and so on. Hence the letter “o” of the plaintext should read in the ciphertext “A”, which corresponds to column “o” and row 12 (alphabet “M”) of the table. To decipher the message the receiver needs to know the key. Then he identifies along the row corresponding to each character of the key, the column where the equivalent character of the ciphertext lies. The lowercase letter in the top row of that column indicates the corresponding letter of the plaintext. Thus in our example, in the row corresponding to the first letter of the key (“M”), the first letter of the ciphertext (“A”) lies in the column “o”.

		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
00	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

**Figure 2.3** – The Vigenère polyalphabetic cipher allowed the use of 26 different cipher alphabets for fast encryption/decryption.

Plaintext:	<b>once upon a time</b>
Key:	<b>MJGM CDTM J GMCD</b>
Ciphertext:	<b>AWIQ WSHZ J ZUOH</b>

**Figure 2.4** – Cryptogram using the Vigenère polyalphabetic cipher with the key “MJGMCDT”.

The advantage of polyalphabetic ciphers was that they guaranteed the security of the encrypted information against a potential frequency analysis, since the same letter was encrypted by a different letter each time. However, polyalphabetic ciphers were slower and much more complex to use than their predecessors, which made them less practical for most applications, particularly when a large number of encrypted messages needed to be sent. Therefore, cryptographers tried to find a cipher harder to crack than monoalphabetic ciphers but easier to implement than polyalphabetic ciphers. The result was the *homophonic substitution cipher*, where each letter is replaced with a variety of substitutes, the number of which must be proportional to the rate of repetition of the particular letter in the language being used. Although this cipher was much more secure than a monoalphabetic one, it was also breakable. In fact, every new “unbreakable” cipher was successively broken with much or less effort. A comprehensive review of the historical development of cryptographic methods can be found in [Singh, 1999].

It was not until 1917 that a true *unbreakable* code was proposed. It is called the *one-time pad* and was invented by an AT&T Bell Labs engineer, Gilbert Vernam (the United States patent #1310719 was issued to him in 1919 [Vernam, 1919]). Using this technique a binary conversion of the message is first performed. The key is another binary sequence that must be as long as the message. To generate the ciphertext the sender has to add modulo 2—exclusive-OR (XOR) logical operation—each bit of the plaintext with the corresponding bit of the key. The receiver decrypts the message (recovers the plaintext) by combining (adding modulo 2) each bit of the ciphertext with the corresponding bit of the key. Using the one-time pad, also known as the *Vernam cipher*, the ciphertext does not contain any patterns from the plaintext nor gives any information about the plaintext to a cryptanalyst. It is secure, provided the key is as long as the message, truly random and used only once.

Its security lies in the randomness of the resulting ciphertext. Notice that if the key of a Vernam cipher is a random stream of bits, then the ciphertext is random even if the plaintext is not random [Salomon, 2006]. Indeed, it is the only mathematically proven secure technique of encryption (see [Shannon, 1948] and [Shannon, 1949b]).

However, the one-time pad assumes that *Alice* and *Bob* (as sender and receiver are commonly known in cryptography) share a secret random sequence of bits, i.e., the key. Therefore, the security of a communication ciphered with the one-time pad depends upon the security of the key distribution process. However, there is no guarantee with classical key distribution schemes (for instance with carriers) that an eavesdropper cannot make a copy of the key during the distribution process.

To overcome this problem public key cryptography was invented. It is a completely new approach, which uses two cryptographic keys, a public key and a private key. The former is used for encryption and it is publicly announced (e.g., published in a website), whereas the latter is used for decryption and has to be kept secret. These two keys are interconnected via a *one-way function*, which is easy to compute in one way (to obtain the public key from the private key) but extremely hard to compute in the opposite way (to extract the private key from the public key).

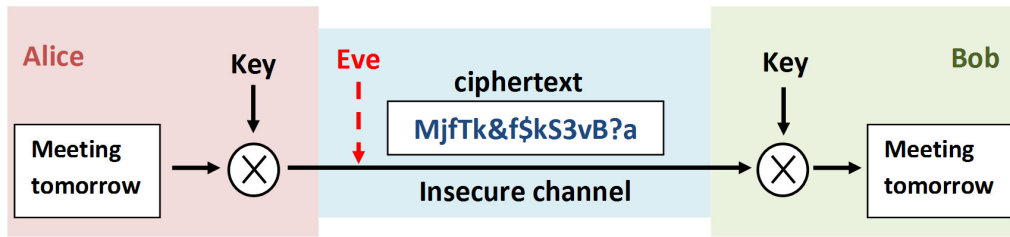
In the following subsections the fundamentals of the two major branches in which classical cryptography can be divided in, namely *secret key* or *symmetric* cryptography and *public key* or *asymmetric* cryptography, are briefly outlined.

### 2.1.1 Symmetric ciphers. The problem of key distribution

Secret key or symmetric cryptography is the traditional and most intuitive scheme for secure communications, in which two parties both encrypt and decrypt their messages using the same shared secret key. This scheme is represented in Figure 2.5. A sender, *Alice*, uses a secure key that must be shared with the receiver, *Bob*, to encrypt a message. The obtained ciphertext is then transmitted through an insecure channel and decrypted by *Bob* using the same shared key. The processes of encryption and decryption are symmetric and hence the name of this type of ciphers. An eavesdropper, commonly known

as Eve, attempting to gain information about the message, may perform some attacks on the communication channel between Alice and Bob to obtain some estimation of the plaintext and also of the encryption key.

Secret key cryptography is subdivided into two fundamental groups depending on the number of characters encrypted: *stream ciphers* and *block ciphers*. In the former, each bit of the plaintext is encrypted individually, while in block ciphers a transformation is made with a group of characters of the original message. Stream ciphers are widely used in communication protocols, as the A5 used in GSM (Global System for Mobile communications) or the E0 generator used in Bluetooth technology.



**Figure 2.5** – Scheme of a symmetric cryptographic transmission where a message is encrypted using a secret key. The obtained ciphertext is transmitted over an insecure channel and decrypted by means of the same secret key shared by the transmitter and the receiver. Eve monitors the channel to try to gain information about both key and message.

Among the developed block ciphers only three of them have been released as public standards: the Data Encryption Standard (DES), later known as DEA (Data Encryption Algorithm) and now superseded since it is not secure due to insufficiently long keys (it could be cracked on a dedicated hardware in less than 24 hours); the TDEA (Triple DEA), which uses blocks of 64 bits with keys of 56, 112 and 128 bits; and the AES (Advanced Encryption Standard), which uses 128-bits blocks with keys of 128, 192 and 256 bits. A comprehensive review of the characteristics of symmetric ciphers can be found in [Fúster et al., 2012, Ch.3].

### 2.1.2 Asymmetric ciphers

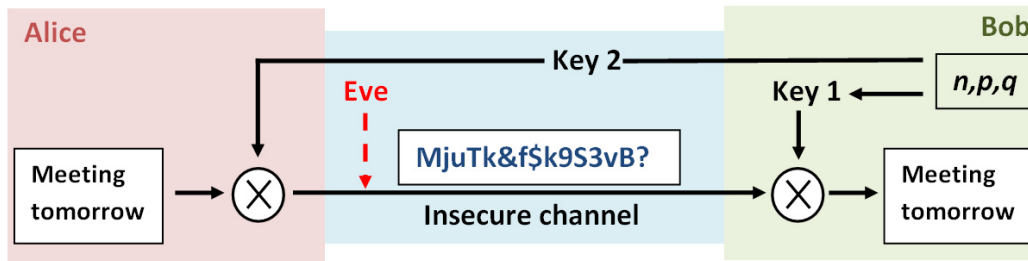
Public key or asymmetric cryptography allows two parties who have never met before to communicate securely. The fundamental difference with secret key cryptography is that in public key cryptography there is no need for sharing a secret key between the parties prior to communication. In this case each party possesses a private key, which is always kept secret, and a public key, which is freely distributed.

The principle of asymmetric cryptography was first proposed in [Diffie et al., 1976] by Whitfield Diffie and Martin Hellman, who were then graduate student and professor at Stanford University, respectively. The Diffie-Hellman (DH) key exchange algorithm is a method for securely sharing a secret key between two parties over an untrusted channel. This key can then be used to cipher a message using a symmetric cipher. The first practical cipher based on public key cryptography was developed by Rivest, Shamir and Adleman from the Massachusetts Institute of Technology [Rivest et al., 1978]. It is known as RSA and even today it is widely used. If one party, say Bob, wants to receive messages encrypted with RSA, he must first choose a private key, which remains secret. Then he generates a public key from the private key and sends it openly to Alice, who uses it to encrypt her message. She then transmits the ciphertext to Bob, who decrypts it with his corresponding private key. A scheme of a generic asymmetric cryptographic transmission is depicted in Figure 2.6. Mathematically it is done the following way, as explained in [Fúster et al., 2012, Ch.7]:

1. Bob generates two large prime numbers,  $p$  and  $q$ , of similar bit-length, and computes  $n = p \cdot q$  and the Euler's totient function of  $n$ , that is,  $\phi(n) = (p - 1)(q - 1)$ .
2. He chooses a positive integer  $e$  between 2 and  $\phi(n)$ , and prime with  $\phi(n)$ .
3. He determines, usually by using the extended Euclidean algorithm, the multiplicative inverse of  $e \bmod \phi(n)$ ,  $d$ , that is, the only integer  $1 < d < \phi(n)$  such that  $e \cdot d \equiv 1 \pmod{\phi(n)}$ .
4. Bob's public key is the pair  $(n, e)$  (represented as Key 2 in Figure 2.6), and  $d$  is his private key (Key 1).

If Alice wants to send an encrypted message to Bob, she must first obtain Key 2 from Bob (his public  $key(n, e)$ ). Then, she codifies the message as an integer  $m$  such that  $0 \leq m < n$ . Finally, she computes the ciphertext  $c = m^e \pmod{n}$  and sends it to Bob. Bob can recover the message (decryption process) by computing  $m = c^d \pmod{n}$ .

Key distribution schemes based on public key cryptography, such as RSA or Diffie-Hellman, have become very popular over the last 20 years and are currently widely employed to establish a secret key over an insecure channel.



**Figure 2.6** – Scheme of an asymmetric cryptographic communication, where Bob generates his private key (Key 1) and public key (Key 2). The latter is sent publicly to Alice who uses it to encrypt a message. The ciphertext is transmitted over an insecure channel and is decrypted by Bob using Key 1. Eve monitors the channel to try to gain information about the message.

### 2.1.3 Security of classical Cryptography. The threat of quantum computing

In nowadays communications both symmetric and asymmetric ciphers are commonly used together. The public keys used by the cryptographic protocols implemented on the internet are certified by established authorities, known as *certificate authorities* (CA), which confirm through signatures that a particular public key certainly corresponds to a given party. Then a cipher based on public key cryptography can be used to exchange a secret key with that party. Subsequently this secret key may be used in a symmetric cipher to transmit encrypted data. The security of this suite of cryptographic protocols relies on the strength of symmetric ciphers, and on the use of one-way functions.

However, it has not still been proven that reversing such one-way functions without the information that is kept secret will always be computationally demanding. Future mathematical advances or in computer science may put a threat in such approaches.

The only unconditionally secure encryption scheme is the one-time pad, a secret key algorithm. No restriction is made about computational power or scientific progress available to break it. Nevertheless, in spite of the existence of a secret key scheme perfectly secure against an attacker with arbitrary computational power, symmetric ciphers have a major practical disadvantage: before two parties can communicate securely they must somehow establish a secret key. This is related to the well-known Kerckhoff's principle, which states that the security of a cryptographic system should not rely on the secrecy of the algorithm used for encryption and decryption, but on the secrecy of the key [Cobourne, 2011]. That is, confidence in a cryptosystem increases when it is public and can be critically analysed by experts that search for security weaknesses.

The security of public key cryptosystems is currently based on the computational difficulty to solve certain mathematical functions, such as the factorisation of large integers or the discrete logarithm problem. This means that public key cryptography algorithms are potentially vulnerable to improvements in computational power or the discovery of more efficient algorithms to solve the mentioned one-way functions. Indeed, algorithms that perform integer factorisation and solve the discrete logarithm problem in polynomial time—rather than exponential—on a quantum computer have already been proposed [Shor, 1997], [Bruß et al., 2007], and have experimentally been tested in [Vandersypen et al., 2001], whereby a nuclear magnetic resonance quantum computer was capable of factorising the number 15 into its prime factors 3 and 5. Although the question about the possibility that a quantum computer of a practical useful size will ever be built or an efficient classical factorisation algorithm ever be found is still open, it is obvious that the threat against current public key cryptography is considerably serious (potentially catastrophic), and therefore a more secure method to ensure communications is needed.



### 2.1.4 The birth of Quantum Cryptography

Quantum Cryptography (QC) is the synthesis of quantum mechanics and cryptography. It was first proposed around 1970 when Stephen Wiesner wrote an unpublished manuscript, where he introduced the concept of *quantum conjugate coding*. The idea consisted in using two conjugate variables to encrypt a message. Conjugate variables such as energy and time, position and momentum or linear and circular polarisations, have associated quantum observables that do not commute, i.e., they cannot have well defined values simultaneously. Although the paper was originally rejected, it was finally published in [Wiesner, 1983], a year before the publication of the well-known paper of Charles Bennett and Gilles Brassard [Bennett et al., 1984].

Quantum cryptography makes use of the laws of quantum mechanics, such as the Heisenberg uncertainty principle and the *no-cloning theorem*, which states that a *qubit* (a quantum bit) cannot be copied or amplified without disturbing its original state [Wootters et al., 1982]. These two principles are the main ingredients of quantum key distribution, which allows Alice and Bob to share a secret random string of bits or cryptographic key, and in conjunction with the one-time pad enables secure communication over an insecure channel. Any disturbance on the qubits caused by an eavesdropper will be detected by the legitimate users.

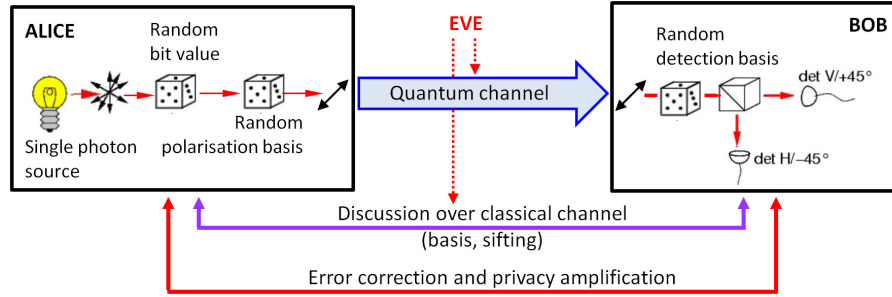
## 2.2 Quantum Key Distribution protocols

The main goal of a QKD protocol is the generation and distribution of a secret key that will be used for encryption. Basically a QKD system involves Alice, Bob and a quantum communication channel. Both parties have also access to a classical insecure communication channel for post-processing purposes. This is schematically shown in Figure 2.7. An eavesdropper is assumed to have access to both channels and no restrictive assumptions are made about the resources at his disposal.

The bits of the key are individually encoded in states of a quantum system, as for instance in polarisation states of single photons, and then distributed between the legitimate parties. Any eavesdropper's attempt to intercept bits



of the key implies that some measurements will be performed on the quantum system, unavoidably changing its quantum state and therefore introducing errors. These errors allow the detection of the eavesdropper. If the error rate is above a certain threshold, the key is considered insecure and it is dismissed.



**Figure 2.7** – Example of a cryptographic system based on quantum key distribution.

### 2.2.1 Classification of QKD protocols

Although there is a wide number of QKD protocols, in [Scarani et al., 2009a] all possible variety of protocols is classified into three main families:

**Discrete-variable protocols**, such as BB84 [Bennett et al., 1984], BBM [Bennett et al., 1992b], E91 [Ekert, 1991], SARG04 [Acín et al., 2004], [Scarani et al., 2004], the six-state protocol [Bennett et al., 1984], [Bruß, 1998], [Bechmann-Pasquinucci et al., 1999] or the B92 [Bennett, 1992].

**Continuous-variable protocols**, either with gaussian modulation, like those proposed in [Cerf et al., 2001], [Grosshans et al., 2002], [Weedbrook et al., 2004] or [García-Patrón, 2007], or with discrete modulation [Silberhorn et al., 2002].

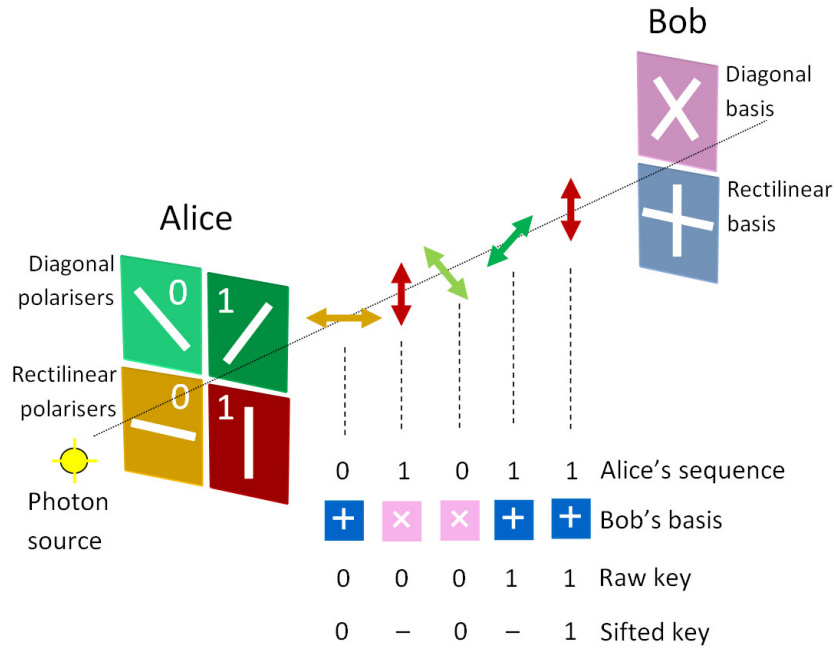
**Distributed-phase-reference protocols**, such as Differential Phase Shift (DPS) reported in [Inoue et al., 2002] or [Inoue et al., 2003], and Coherent One Way (COW) [Gisin et al., 2004], [Stucki et al., 2005].

Other works classify the protocols according to different criteria, like in [Martínez-Mateo, 2008] where they are categorised in protocols based on *non-orthogonal states* and protocols based on *entangled states*.

Discrete-variable coding is the original coding scheme, first published by Bennett and Brassard in 1984. This type of QKD protocols is still the most frequently implemented. In the following, the most popular of those protocols are briefly described.

### 2.2.2 The BB84 protocol

As mentioned above, in 1984 Bennett from IBM and Brassard from the University of Montreal proposed the first QKD protocol. This protocol is called BB84 and uses four quantum states to encode the bits of a cryptographic key. For the polarisation-coding version, these quantum states are four polarisation states: vertical, horizontal,  $+45^\circ$  and  $-45^\circ$ , which form two conjugate bases (rectilinear and diagonal). The procedure of the BB84 protocol is as follows [Zbinden et al., 1998]:



**Figure 2.8** – Schematic view of the BB84 protocol. Alice sends a sequence of bits encoded in photons with random polarisation: horizontal, vertical,  $+45^\circ$  or  $-45^\circ$  (row 1). Bob randomly chooses either his diagonal or his rectilinear detector basis (row 2) and records the results of his measurements (row 3). Finally, Alice and Bob compare the bases they used and retain the results with compatible bases, obtaining the sifted key (row 4).

1. Quantum communication phase:

- (a) Alice sends Bob a sequence of independently randomly polarised photons. As above mentioned, four possible polarisations are used (see Figure 2.8).
- (b) For each received photon, Bob randomly uses one of the two conjugate bases (rectilinear or diagonal) to make a measurement.
- (c) Bob records the bases he used and the results, these last called *raw key*. Then he publicly acknowledges that he has received the signals.

2. Public discussion phase:

- (a) Alice broadcasts the bases she used to polarise each photon sent. Bob broadcasts the bases he used to perform each measurement.
- (b) Alice and Bob discard all bits corresponding to events where they used different bases. The resulting string is called the *sifted key*.
- (c) To test for eavesdropping Alice randomly chooses as *test events* a fraction of the remaining events and publicly broadcasts their positions and polarisations.
- (d) Bob broadcasts the polarisations of the test events too.
- (e) Alice and Bob compute the error of the test events, that is, the fraction of bits for which their value disagree. If the error rate exceeds an established threshold value (around 11%) [Lütkenhaus, 2000], the protocol is aborted. Otherwise, they continue to the last steps.
- (f) Alice and Bob each generate a binary string from the polarisation information of the remaining data. At last, to generate a final secret key they can perform classical protocols such as *error correction* and *privacy amplification*, which will be briefly commented in section 2.2.4.

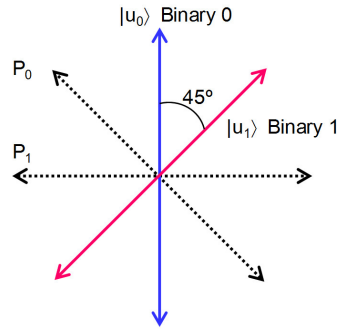
If Eve tries to eavesdrop the key right after Alice has sent the string of photons, she has to randomly guess the basis to detect each photon since she ignores both, the bases used by Alice to prepare the photons and the bases

in which Bob is going to detect them. After detection Eve has to regenerate the photons in the bases she has chosen with the bit values she has obtained and send them to Bob. The bases chosen by Eve will be with 50% probability different from Alice's bases. Eve does not introduce any error if she uses the same basis as Alice used, since in the case that Bob measures correctly, Eve used the same basis as both of them, and if Bob does not use the correct basis, the result is then discarded. This happens with 50% probability. If Eve does not use the same basis as Alice (the remaining 50%), the photon will still be recorded by Bob correctly 50% of the time. Thus, the increased error rate introduced by Eve if she intercepts and resends every photon in the transmission is on average of 25%. As mentioned above, Alice and Bob compute the error rate by publicly comparing a subset of the sifted key. Error rates exceeding a secure pre-established limit reveal eavesdropping.

It should be stressed that the classical communication channel between Alice and Bob must be authenticated. Otherwise, Eve could easily perform a *man-in-the-middle attack* by acting as Alice to Bob and as Bob to Alice. Recently a method for quantum authentication has been experimentally demonstrated for the first time [Clarke et al., 2012].

### 2.2.3 The B92 protocol

The B92 protocol proposed in [Bennett, 1992] is basically a simplified variation of the BB84 protocol. The main difference is that only two non-orthogonal states rather than four are necessary in the B92 protocol to guarantee the security of a QKD system. This security depends on the indistinguishability of non-orthogonal quantum states and the inevitable perturbation arising from measurements performed on these states when the sequence of encoding states is unknown to an eavesdropper. In the QKD system investigated in this thesis, the B92 protocol was implemented using two non-orthogonal polarisation states of single photons, say  $|u_0\rangle$  and  $|u_1\rangle$ , associated with the bit values 0 and 1 respectively, as shown in Figure 2.9. At the receiver two projection operators  $P_0$  and  $P_1$ , orthogonal to  $|u_1\rangle$  and  $|u_0\rangle$  respectively, are used. In practice these projection operators can be implemented with two polarisers (see Figure 2.10).

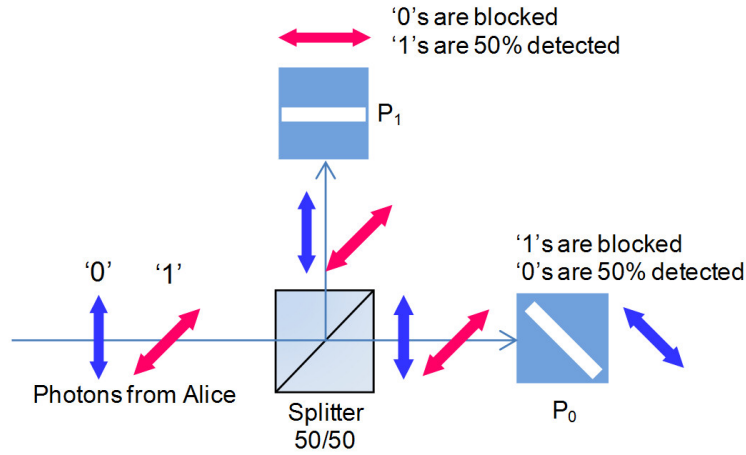


**Figure 2.9** – Example of B92 photon polarisation and bit encoding.

Similarly to the BB84 protocol, Alice sends a string of photons randomly encoding the binary values ‘0’ and ‘1’ with two linearly polarised quantum states at a relative angle of  $45^\circ$ . Bob performs measurements of qubits with either of two polarisers (see Figure 2.10), which sometimes fail (the polariser of each channel is oriented to block the unwanted polarisation state in that channel), but when a measurement succeeds it always provides the bit value correctly —note that under these measurement scheme if Alice transmits a ‘0’ the probability of Bob detecting a ‘1’ is minimal. That is, Bob still randomly chooses a basis for each photon measurement but if he chooses the wrong basis, he will not measure anything. Thus there is no need for reconciliation of basis sets between Alice and Bob to discriminate ambiguous measurements; the string measured by Bob is directly the sifted key, what simplifies this protocol when compared to the BB84 protocol. Bob only tells Alice in which instances he measured a photon (but not, obviously, if this was a ‘1’ or a ‘0’).

The fact that two non-orthogonal quantum states can be unambiguously distinguished at the cost of some loss was first proven in [Ivanovic, 1987]. The fraction of the bits sent by Alice that Bob can measure unambiguously is given by  $I_{AB} = (1 - \cos \alpha)$ ,  $\alpha$  being the angle formed by the non-orthogonal polarisation states. The maximum of this fraction corresponds to 29% [Clarke et al., 2001] for a relative angle  $\alpha$  of  $45^\circ$ . If Eve intercepts the stream of photons from Alice and performs measurements on them, she will introduce a loss in the sequence of photons she resends to Bob. This loss corresponds to 71% of the signal for a relative angle of  $45^\circ$ , an amount that, in principle, is detectable by Alice and Bob. However, the B92 protocol exhibits a security

weakness not present in the BB84 protocol: if the loss of the channel is higher or equal to 71%, Eve's presence would remain unnoticed if she compensates all the loss she causes by replacing the normal 'lossy' channel by a 'lossless' one. This attack (the *unambiguous state discrimination* strategy) will be discussed in subsection 2.4.3.



**Figure 2.10** – Experimental scheme at Bob for the detection of two non-orthogonal polarisation states '0' and '1'.  $P_0$  and  $P_1$  are two polarisers that perform projection measurements and are oriented to block the unwanted state in that channel.

The B92 protocol with two non-orthogonal polarisation states above described is a variation of the original B92 protocol [Bennett, 1992], which uses two non-orthogonal coherent states. The unconditional security of the original B92 has been proved in [Tamaki et al., 2004], [Tamaki et al., 2003], and for some implementations with a strong reference pulse in [Koashi, 2004], [Tamaki et al., 2009].

#### 2.2.4 Error correction and privacy amplification

After Alice and Bob perform the basis reconciliation step of the BB84 protocol they obtain the sifted key, which may still contain errors. Low error rates are indicative of nothing more serious than noise and physical imperfections in the devices. However, even these small errors can cause erroneous encryption

and/or decryption of information. Therefore error correcting the keys resulting from even the highest fidelity key exchanges is necessary.

Shannon's information theory gives the theoretical minimum amount of public information that must be exchanged to correct the errors of a given message. This quantity of information is given by the binary entropy function of the quantum bit error rate of the sifted key [Shannon, 1949a]. Brassard and Salvail discussed several error correction codes in their work [Brassard et al., 1994] before deciding the protocol entitled "Cascade" was an efficient method for correcting errors.

The Cascade scheme is an iterative process whereby Alice and Bob divide the sifted key into blocks. The parity of each block is then compared across a public channel with those of even parity being accepted as error-free whilst those of odd parity are subjected to further subdivision and comparison until the error is found and corrected. Any errors that occurred in the even parity blocks are detected and corrected by repeating the process several times with different block sizes and permutations. The process continues until Alice and Bob are sure that their sifted keys are identical.

*Privacy amplification* is the term given to the process of distilling a highly secret key from a partially compromised bit string and is a required further step in the key reconciliation process. This is due to information leakage, which occurs as a result of the key exchange and error correction processes. The amount of information that an eavesdropper may have depends upon factors such as the eavesdropping strategy used, the error rate and the error correction scheme used by Alice and Bob.

A typical privacy amplification process works as follows. Alice and Bob apply a XOR operation to random pairs of bits. This time they do not announce the operation results publicly. Instead they announce the positions in the string of bits they used and they replace the two bits by their XOR value. Hence, Eve cannot interact in this process and her information will be reduced to an arbitrarily small amount that Alice and Bob decide.

## 2.3 Components in a QKD system

A typical QKD system can be divided into three parts: the transmitter, whose main purpose is to emit individual photons with associated conjugate variables encoding a random sequence of bits; the quantum channel, which is the transmission medium between emitter and receiver, and whose fundamental role is to preserve the quantum states of the photons; and the receiver, which detects single photons and randomly analyses their quantum states.

### 2.3.1 Transmitter. Emission of single photons

The main function of the transmitter of a QKD system consists in sending single photons to the receiver, each carrying one bit of information. For that purpose the transmitter would ideally use single-photon sources, i.e., a device that would generate exactly one photon when required. However, the technology of single-photon emitters is still not sufficiently matured to permit high transmission rates, and therefore the “single-photon regime” is generally achieved by strongly attenuating a pulsed laser. This technique is known as Weak Coherent Pulses (WCP) and ensures that the probability of having more than one photon in a laser pulse becomes negligible.

This approximation has two disadvantages due to its characteristic Poisson distribution. One affects the transmission rate, since the vacuum probability is much higher than the probability of emitting a photon, so most of the pulses are empty with the consequent decrease in the transmission bit rates. The other concerns the security of the key, since the probability of more than one photon in a laser pulse is always nonzero, thus an eavesdropper could perform a *photon-number splitting attack* (see subsection 2.4.3). However, protocols with attenuated coherent states that implement techniques such as *decoy states*, which counteract this type of attacks achieving equivalent security levels to those obtained with single-photon emitters, have already been reported [Hwang, 2003], [Lo et al., 2005]. Moreover, these protocols allow the use of higher mean photon numbers per pulse, and hence higher transmission rates, maintaining the security level. Therefore, due to their simplicity WCPs have been used in the majority of QKD systems to achieve the single-photon



regime, since just an attenuator and a laser source are sufficient for their realisation.

When a laser emission is attenuated to an average number of photons per pulse  $\mu$ , the probability of finding  $n$  photons in any pulse is given by Poisson distribution:

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu} . \quad (2.1)$$

Using equation 2.1, the probability of finding more than one photon in a non-empty pulse can be calculated as:

$$P(n > 1 | n > 0, \mu) = \frac{1 - P(0, \mu) - P(1, \mu)}{1 - P(0, \mu)} = \frac{1 - e^{-\mu}(1 + \mu)}{1 - e^{-\mu}} \cong \frac{\mu}{2} . \quad (2.2)$$

Consequently, there is always a nonzero probability of finding more than one photon in a pulse. Decreasing  $\mu$  decreases this probability; however it also decreases the transmission rate. The choice of  $\mu$  is the subject of considerable work [Lütkenhaus, 2000] and is determined by the characteristics of the system.

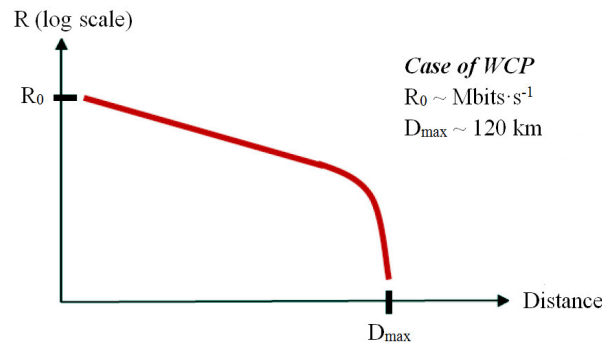
Another method of approximating single photons is the generation of photon pairs by parametric downconversion [Kwiat et al., 1995], [Weinfurter, 2005]. This phenomenon consists in the generation of two entangled photons when a laser beam pumps a nonlinear crystal. One of the photons is used as the trigger for the second photon [Hong et al., 1986]. This technique has the disadvantage of a highly inefficient photon-pair creation process, typically one photon pair per  $10^{10}$  pump photons [Gisin et al., 2002], so it is only worth substituting faint laser pulses for this technique when the entanglement of the photons is going to be exploited.

### 2.3.2 Channel: optical fibre or free space

A quantum channel can be any medium where light can propagate, although it should be clarified that what is quantum is the information, not the channel itself. Any quantum channel should ideally have low loss and should preserve the quantum states, avoiding de-coherence from the environment. There are two types of channels with these properties: optical fibre and free space.

Optical fibres are used in the already available commercial QKD systems, and also in many scientific experimental setups [Hughes et al., 1999],

[Tang et al., 2009]. The reason for that may lie in the fact that a fibre-based quantum channel, when compared to a free-space one, is not affected by external factors such as weather conditions, solar background radiation, or the fact that free-space QKD usually requires the implementation of ancillary techniques such as automatic tracking to maintain the alignment of the link. However, optical fibres present some disadvantages too, such as their birefringence [Agrawal, 2002]. Birefringence in optical fibres makes polarisation coding-based QKD systems harder to implement, since it degrades the polarisation of the quantum states and a compensation method is essential, such as ‘*plug and play*’ QKD [Zbinden et al., 1997], [Stucki et al., 2001]. Moreover, the loss in optical fibres limits the longest achievable distance for a fibre-based QKD system (typically limited to about 200 km [Gobby et al., 2004]). Figure 2.11 shows the bit transfer rate plotted against distance travelled along a fibre-based quantum channel.



**Figure 2.11** – Typical profile of the Rate versus Distance curve for a fibre-based QKD link (after [Dianati et al., 2008]).

As can be observed in the figure, the negative slope of the curve becomes steeper at a certain distance, and at approximately 120 km the signal disappears. This is due to the impossibility of amplifying and regenerating the qubits without perturbing the quantum states and therefore increasing the error rate [Li et al., 2007]. Much research is being done in an attempt to extend this distance, for example in [Stucki et al., 2009] by using ultra low loss optical fibres, or in [Scherer et al., 2011], where a non-perturbative theory for practical QKD based on entanglement swapping is proposed. However, it is yet a limiting factor in the potential deployment of quantum channels using

optical fibres. Moreover, due to the impossibility of amplifying quantum bits, it is not clear whether the installed fibre infrastructure can be easily used for QKD.

Free-space quantum communications, on the other hand, will play an important role in securing satellite-based global communications as well as reducing the ‘connectivity bottleneck’ affecting metropolitan optical networks [Willebrand et al., 2002]. A very important advantage of sending photons through the atmosphere is that this medium is essentially nonbirefringent, thus facilitating the use of polarisation coding. Moreover, free-space links have negligible dispersion on polarisation and frequency. In addition, transmission over long distances can be enhanced by selecting the appropriate wavelength of the photons. Indeed the atmosphere has a high transmission window in the vicinity of 850 nm, what is compatible with commercially available silicon Avalanche Photo Diodes (APDs) photon-counting modules, which can have detection efficiencies as high as 65%.

The emitter and receiver are usually connected in free space by two telescopes pointing at each other. Although it may seem difficult to detect single photons amidst background light, the first experiments already demonstrated the feasibility of free-space QKD over laboratory [Bennett et al., 1992a], [Buttler et al., 1998b], and over modest outdoor distances [Jacobs et al., 1996], [Buttler et al., 1998a], [Hughes et al., 2000]. The contribution of background radiation to the error rate can be kept reasonably low by using a combination of software filtering (selecting only the photons detected in a determined time window from the bit period), spectral filtering (by using narrow interference filters  $\leq 1$  nm), and spatial filtering (‘cleaning’ the beam from higher spatial modes and other surrounding areas outside the laser beam by passing it through sufficiently small apertures), what is further discussed in section 5.8 of this thesis.

Finally, the performance of free-space QKD systems depends on atmospheric conditions and air quality, which can be more noticeable in urban locations where pollution and aerosols degrade the transparency of the air.

### 2.3.3 Receiver. Detection of single photons

The receiver of a QKD system should be capable of detecting single photons, since each single photon carries one bit of information. Single-photon detection can be achieved by using different devices such as PhotoMultiplier Tubes (PMT), micro channel plates, superconducting Josephson junctions, Single-Photon Avalanche Diodes (SPAD), Superconducting Single-Photon Detectors (SSPD), among others [Fernández-Mármol, 2006, §3.7.2]. An ideal detector for a QKD system should have good detection efficiency, low dark noise, low timing jitter and low dead time. SPADs have been used as single-photon detectors in the majority of the QKD systems built to date due to their high efficiency and low noise equivalent power.

The characteristics of single-photon detectors have a significant bearing on the overall system performance of the QKD system that employs them. In [Clarke et al., 2011] a phase-encoded QKD system is used to compare the performance of different types of single-photon detectors and to analyse their influence on the final key exchange rate. The detectors studied were thick-junction Si-SPADs, two different thin-junction Si-SPADs, a resonant cavity thin-junction Si-SPADs and a niobium nitride nanowire SSPD. A theoretical model of the experimental system was also developed to understand the combination of the detector parameters that are desirable for efficient QKD, and to predict the behaviour of the system with hypothetical realistic detectors and evolutions of existing detectors. For instance, the theoretical model predicts that for the reported system a better net bit rate can be achieved by using PerkinElmer thick-junction Si-SPADs with 42% detection efficiency, 198 dark counts per second and pulse read out electronics modified to give a Full-Width at Half-Maximum (FWHM) timing jitter of 200 ps, than with 62 ps FWHM timing jitter SSPDs with 10% detection efficiency and 10 dark counts per second, at distances of up to 15 km and clock frequencies up to 1 GHz. At higher clock frequencies the system suffered from intersymbol interference, which increased the error rate that could be obtained with the PerkinElmer thick-junction Si-SPAD and thus reducing the net bit rate.

The principle of operation of SPADs and their choice as the detectors for the system investigated in this thesis will be discussed in section 5.3, comparing their general features to those of other single-photon detectors.

## 2.4 Security of QKD

In this section the security of real-life QKD implementations is discussed. The quantum bit error rate (QBER) plays a fundamental role in assessing the security of a QKD system, and thus the definition of this figure of merit is first presented. Next, both the security strengths and weaknesses of QKD are described, including a revision of the most important eavesdropping strategies. Finally, a new form of quantum cryptography, the so-called *device-independent quantum key distribution*, is discussed.

### 2.4.1 Quantum bit error rate

The analysis of the QBER allows the authorised parties of a QKD system to detect the possible presence of an eavesdropper in the transmission channel. As already mentioned in section 2.2, Alice and Bob publicly broadcast the bit values of a fraction of the sifted key —referred to as test events— and compute their error rate to check for eavesdropping. If the error rate is larger than an agreed threshold value above which the key transmission is considered as insecure (since all errors must be attributed to the presence of an eavesdropper), Alice and Bob discard the key and start a new exchange protocol. The QBER is generally expressed as the ratio of wrong events (events for which Alice and Bob's values disagree) to the total number of received events:

$$QBER = \frac{N_{wrong}}{N_{wrong} + N_{correct}}. \quad (2.3)$$

The errors in a free-space QKD system typically arise from three sources. The first one is an error rate that results from imperfections in the optics of the system and is equivalent to the fraction of photons, the polarisation or phase of which is erroneously determined. This source of error can be characterised by measuring the polarisation extinction ratio of the quantum states for a polarisation-encoding QKD system or the classical fringe visibility  $V$  for a phase-based QKD system [Mansuripur, 2002, Ch.24]. The second source is the timing jitter of the QKD system, which may cause *intersymbol interference*, as will be discussed in section 6.3.1. Finally, the third source of error in a

QKD system is due to the noise present in the single-photon detectors, which in turn can be originated intrinsically in the detectors, i.e., the dark counts, or arise from external sources such as the solar background radiation. It is usually accepted that the QBER must be under a value of  $\sim 11\%$  —or less, depending on the actual protocol and implementation— to guarantee that an eavesdropper has not tapped the channel [Lütkenhaus, 2000], [Brassard et al., 2000].

### 2.4.2 Security foundations of QKD

Unlike conventional cryptography, QKD bases its security on the fundamental laws of Physics: the no-cloning theorem and Heisenberg’s uncertainty principle. Furthermore, the security provided by QKD is guaranteed in the event of a future attack, unlike current public key cryptography, which can leave sensible information exposed in a future scenario involving a quantum computer attack [Shor, 1994]. The security of QKD has been proven in several studies [Shor et al., 2000], [Mayers, 2001] (even considering a noisy channel [Lo et al., 1999]). However, some assumptions were made, such as the physical security of encrypting/decrypting devices, a true source of random numbers, an authenticated classical channel between both users, reliable single-photon emitters and detectors, and all parties operating within the laws of Physics. In [Wang, 2006] the unconditional security of the standard BB84 protocol is demonstrated even when an imperfect source such as coherent light from a laser is used. The security proof of this protocol was obtained based on the virtual entanglement purification by classical hashing.

Regarding true sources of random numbers, the feasibility of using a physical random bit generator with chaotic semiconductor lasers in a high-speed QKD system is described in [Honjo et al., 2009].

The assumption that all parties operate under the laws of Physics requires that any eavesdropper be bounded by the laws of quantum mechanics. No further restrictions apart from the eavesdropper’s inability to access the devices are made. In particular, the eavesdropper is allowed to have arbitrarily large quantum computing technology, far more powerful than the current state of the art.

Secure authentication is one of the most important aspects to consider when evaluating QKD security. In order to be protected against man-in-the-middle attacks, the classical communication that takes place in QKD must be authenticated. Digital signatures are widely used in current communication networks to verify the origin and authenticity of messages. These digital signatures are usually based on the already mentioned one-way functions used in public key cryptography, thus they are not secure for the same reason as public key cryptography is not secure: the difficulty to reverse such functions without the secret information has never been mathematically proven. Quantum digital signatures (QDS), on the other hand, promise authentication verified by information-theoretical limits and quantum mechanics [Clarke et al., 2012].

The assumption about the reliability of the physical devices is one of the main weaknesses of QKD and is deeply discussed in the following section. This is due to the physical imperfections of the devices available with current technology that are used for the implementation of QKD [Scarani et al., 2009b]. This was observed with the first prototype of a QKD system, which leaked key information through the power supply used to feed the Pockel cells, making different noises depending on the voltage needed for each polarisation [Brassard, 2005]. This type of attack is commonly referred to as a *side channel attack* and can be very powerful if the vulnerabilities of practical implementations of QKD are not properly characterised and bound.

### 2.4.3 Attacks to QKD systems

When assessing possible eavesdropping techniques it has to be assumed that Eve possesses perfect technology and that she is just limited by the laws of quantum mechanics (the no-cloning theorem) and not by technical obstacles. It must also be considered that all errors derived from a key exchange are caused by Eve. Even if the sources of errors of a QKD system are perfectly characterised, the wrong detections have to be attributed to an eavesdropper perturbation, as Eve could use “error-free” devices and hide the disturbance she causes in them. It must also be assumed that Alice and Bob have available only current technology. In the following the main eavesdropping strategies are reviewed.

### Intercept-resend attack

The simplest eavesdropping strategy is the so-called *intercept resend attack*, where Eve merely intercepts the quantum channel, measures the photons sent by Alice, and resends the states she has measured to Bob. The process in a BB84 implementation would be as follows [Weier, 2003]:

Suppose Alice and Bob measure and receive in the same basis (otherwise the event will be discarded during sifting). Let us assume that Alice sends a horizontal polarisation state (which encrypts the ‘0’ binary value), and Bob has his analyser set to the rectilinear detector basis (see Figure 2.8). If Eve intercepts the photon from Alice and measures the polarisation in the rectilinear basis too, she will measure in the correct basis and therefore she will detect the horizontal polarisation and will transmit it. Bob, who is also using the correct basis, will also measure the horizontal polarisation state. Eve will have measured the bit correctly and she will not have introduced any error. In 50% of the cases, however, Eve will set her analyser to the diagonal basis. As her measurement outcome is random she will transmit a  $45^\circ$  (‘1’) in 50% of the cases and a  $135^\circ$  polarisation (‘0’) in another 50%. Since Bob’s measurement result is random as well, in 50% of those cases (so in total in 25% of all cases) he will measure a vertical polarisation state, that is, the opposite polarisation to the one that Alice sent, in spite of both having used the same basis set. Therefore, Alice and Bob will find a QBER of 25% when an intercept-resend strategy is taking place, alerting them of Eve’s presence.

### Unambiguous state discrimination attack

A special case of an intercept-resend attack is the *unambiguous state discrimination (USD) attack* [Dušek et al., 2006], which can be applied whenever Alice sends linearly independent signal states. In this attack Eve makes an unambiguous state discrimination measurement to each photon [Clarke et al., 2001]. She is then able to detect deterministically 29% of the photons, whereas in the remaining 71% of the cases the measurement is ambiguous. Then, Eve forwards a new photon to Bob in those cases where she knows she measured the bit correctly, while she sends the vacuum state in the remaining cases. It has to be assumed that Eve is able to establish a lossless channel with Bob.



Therefore she can compensate some or all the loss she has caused when she measured the photons from Alice. Since she has caused a loss of 71%, if the loss of the transmission channel is equal or higher than that value, no key can be exchanged between Alice and Bob securely [Tamaki et al., 2003]. If the loss of the transmission channel is lower, Alice and Bob could still distil a secret key, albeit at the cost of discarding the information gained by Eve through privacy amplification. Therefore the B92 protocol is vulnerable to losses in the transmission channel and thus they need to be carefully characterised.

### Quantum cloning attack

Another eavesdropping strategy is the *quantum cloning attack* with a universal quantum cloning machine proposed in [Gisin et al., 1997]. Using this quantum cloning machine Eve *copies* the photons sent by Alice with certain fidelity and keeps the copied photons in a quantum memory. When Alice and Bob announce their bases in the sifting step, Eve can measure her qubits in the correct bases. The introduced error is 16.7%, lower than that of an intercept-resend strategy.

### Optimal eavesdropping attack

An *optimal eavesdropping attack* has been studied in [Fuchs et al., 1997]. It consists in Eve letting a four-dimensional probe (two qubits) interact unitarily with a photon sent by Alice. She then waits until Alice and Bob announce the used basis, and with this information she performs an optimised measurement on the stored probe, depending on the basis. Under the threat of this attack the key exchange must be considered insecure if the QBER exceeds a value of 14.6%.

### Attacks exploiting imperfections of the physical devices

The above described attacks can be performed without any previous consideration about the devices employed in QKD systems. However, the physical imperfections of the components of QKD systems —also called *loopholes*—

open the door to different powerful eavesdropping attacks that exploit such vulnerabilities. Some of them will be described in the following.

Light modulators are vulnerable to a *large pulse attack*, presented in [Vakhitov et al., 2001], whereby Eve sends high-power light pulses to obtain information about the modulator settings, and thus by measuring the characteristics of the reflected pulses she may know the transmission bases, which allow her to detect the quantum states unambiguously. Light modulators can also be attacked with a *phase-remapping* strategy, which is a type of intercept-resend attack introduced in [Fung et al., 2007] and experimentally demonstrated in [Xu et al., 2010], where the mentioned security loophole is exploited in a commercial “plug and play” QKD system. It should be mentioned that this attack introduces a high error rate and is discoverable under most QKD protocols.

Furthermore, the characterisation of the physical channel and the calibration of the cryptosystem hardware are necessary in order to establish a quantum channel. If the calibration routine is not properly implemented, a security loophole can be opened, as pointed out in [Jain et al., 2011b]. In this paper a method to induce a large temporal detector efficiency mismatch in a commercial QKD system is proposed and experimentally demonstrated. This method is known as a *channel calibration attack* and consists in first deceiving a channel length calibration routine and then, elaborating an optimal strategy using faked states to break the security of the cryptosystem.

In the following eavesdropping strategies derived from imperfections in photon emission and detection are described. Due to their serious implication in security, these attacks have drawn considerable attention in the scientific community in the last few years.

### Attacks exploiting imperfections in photon emission

Different vulnerabilities arise from the physical implementation of the emission of photons in practical QKD systems. The use of weak coherent pulses as source of single photons implies a nonzero probability of generating more than one photon in a pulse. Thus an eavesdropper can perform a *photon-number splitting attack* (PNS) [Huttner et al., 1995], [Brassard et al., 2000],

[Lütkenhaus et al., 2002], whereby she suppresses the pulses with only one photon and resends the pulses with more than one photon, having previously kept one copy for herself. To counteract the PNS attack several schemes have been proposed: the non-orthogonal encoding protocol SARG04 [Scarani et al., 2004], the differential phase shift QKD [Inoue et al., 2002], [Feng et al., 2007], or the decoy-state method [Hwang, 2003], [Harrington et al., 2005]. In the decoy-state technique Alice randomly replaces signal pulses (attenuated to emulate the single-photon regime) by multiphoton pulses (decoy-states). Then Alice and Bob compute the *yield*, or the conditional probability that a signal is detected by Bob given that it is emitted by Alice as an  $n$ -photon state, for both the signal states and the decoy-states. If the yield of multiphoton states is abnormally high compared to that of the signal states, then the protocol is aborted since a PNS attack may have taken place.

In plug-and-play systems [Muller et al., 1997] photons do a round trip from Bob to Alice and back to Bob. They are first sent from Bob to Alice, and when they enter Alice's equipment, they get reflected by a Faraday mirror, phase modulated and then sent back to Bob. This configuration makes these systems highly vulnerable to a *Trojan-horse attack* [Gisin et al., 2006], whereby Eve intercepts the channel between Alice and Bob and sends bright pulses to Alice. She then analyses the backscattered light with a detector, whereby she can gain some information about the key. In order to counteract this attack a detector in Alice must be placed to monitor the level of incoming light. In addition, careful filtering and timing, attenuation addition and phase randomization of Alice's apparatus must be implemented, in conjunction with a security proof [Zhao et al., 2008b].

Another problem arises when Alice uses different laser diodes to encode each binary state. They will have different intrinsic properties that make them have different spectra. Careful adjustment of their temperature must be done in order to ensure the same wavelength is emitted by both of them at all times. Even so, the leakage of information should always be characterised and bound.

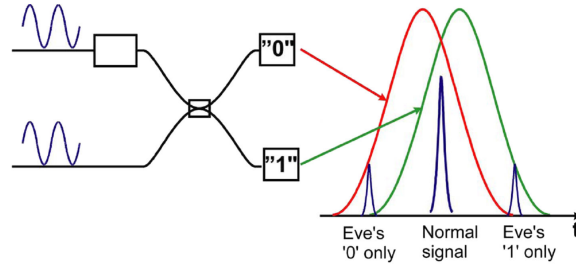
### Attacks exploiting imperfections in photon detection

It is virtually impossible to manufacture identical detectors in practice. Hence, when two or more detectors are used in a QKD system they may exhibit different detection efficiencies depending on a combination of variables such as time, frequency, polarisation, and/or spatial domains [Zhao et al., 2008a]. If Eve manipulates a signal in these variables, she could effectively exploit the detection efficiency loophole to break the security of a QKD system.

Single-photon detectors are sometimes used in the so-called *gated mode*, which is very effective in reducing the background rate and the dark-count rate. When operated in this mode the detector is sensitive to a photon only over a short period of time, which is usually controlled by a bright timing pulse that is launched from Alice preceding each single-photon pulse. In implementations where two detectors are used, one of them is used to detect the ‘1’s and the other to detect the ‘0’s. These two detection windows can be slightly time shifted relative to each other, due to small optical path length differences or delays in the circuitry. Eve can take advantage of this shift, break the line between Alice and Bob, and subsequently generate a *faked states attack* [Makarov et al., 2005], [Makarov et al., 2008], which is a type of intercept-resend attack where she generates her own states and sends them to Bob without alerting of her presence. In particular she manipulates the timing of the pulses encrypting ‘0’ and ‘1’ states by introducing an additional time shift [Makarov et al., 2006]. She makes the ‘0’ states to lie on one extreme of its efficiency curve (see Figure 2.12) so that only detector ‘0’ can ‘see’ this state, and analogously the ‘1’ states on the opposite side of the trace so that only detector ‘1’ will be capable of detecting it. Therefore, since she can control what Bob receives she will resend the states from Alice without being detected. This attack is also known as *time-shift attack*. Some experimental demonstrations of this attack are presented in [Qi et al., 2007] and [Zhao et al., 2008a]. In [Lydersen et al., 2011b] a countermeasure to this attack called *bit-mapped gating* is presented, which is a way to force the detections in the middle of the detector gate by coupling detection time and quantum bit error rate.

Silicon avalanche photodiodes emit fluorescence when an avalanche takes place in the junction upon reception of a photon [Kurtsiefer et al., 2001]. This

light could be sensed by an eavesdropper to assess which detector fired and get information about the key. This attack can be avoided by using other detectors that do not emit this back flashed light, which is discussed in [Collins et al., 2007].



**Figure 2.12** – Efficiency curves showing the mismatch between the states received by Bob’s detectors (after [Makarov et al., 2006]).

Silicon avalanche photodiodes can be “blinded” [Makarov et al., 2009], [Sauge et al., 2011], [Lydersen et al., 2010a] by firing bright pulses at them, typically from 1 to 10 mW at  $\lambda \sim 780$  nm, what is usually known as a *blinding* or *bright illumination attack*. In this mode the detectors are totally insensitive to single photons, but can be externally controlled by an eavesdropper to make them click controllably. In [Makarov et al., 2009] an eavesdropping experimental attack was performed on a commercial QKD system whereby the whole key was obtained without introducing any error. Against bright illumination attacks “monitoring the photocurrent” was proposed as a countermeasure in [Yuan et al., 2011a], which is based on the vast difference in the measured APD currents as compared with normal operation.

However, the debate over the security of QKD against loopholes is intense and very open [Lydersen, 2011], [Yuan et al., 2011b]. The scientific community is divided between two approaches. One approach consists in securing QKD systems by carefully assessing all possible loopholes, and limiting the information leaked to an eavesdropper by an adequate experimental implementation that minimises this information. The other approach consists in developing new protocols and security proofs that are intrinsically secure against these loopholes, such as the decoy state protocol for the PNS attack.

### Experimental demonstrations of eavesdropping attacks

In [Lamas-Linares et al., 2007] it is experimentally demonstrated how an eavesdropper may use the timing information that is revealed during public discussion between Alice and Bob, to have access to a significant portion of the key without being noticed.

The first full-field implementation of a complete faked-state eavesdropping attack on an operating QKD system is described in [Gerhardt et al., 2011]. A fibre link of 290 m was attacked during a few hours, and Eve was able to obtain the same key as Bob from multiple QKD sessions. Eve remained undetected since none of the usual parameters that are monitored during the QKD exchange were disturbed.

In [Lydersen et al., 2010a] the crack by means of the blinding attack of two commercial QKD systems (id3110 Clavis2 from ID Quantique and QPN 5505 from MagiQ Technologies) is demonstrated. The authors showed experimentally how Eve can use bright illumination to blind the gated detectors of the QKD systems. This blinding converts them into classical linear detectors, making them fully controllable by laser pulses superimposed over the bright continuous-wave illumination. Based on these experiments, a detailed proposal about how to attack gated detector with off-the-shelf components by using *thermal blinding* is presented in [Lydersen et al., 2010b].

A technically much simpler but very effective attack, which does not require the interception of the quantum channel, is described and experimentally demonstrated in [Weier et al., 2011] (see also [Weier, 2011]). Without being detected, an eavesdropper can asymptotically obtain complete information about the generated key by just exploiting the dead time of the single-photon detectors. This strategy is called *dead time attack*, whereby Eve was able with very simple equipment to correctly infer up to 98.8% of the key without significantly increasing the QBER. The authors also provide an effective countermeasure against this and similar attacks.

An *after-gate attack* performed on a quantum cryptosystem is presented in [Wiechers et al., 2011]. Bright pulses were used as faked states timed to arrive at the APDs outside the activation time. Then, the authors note that, as faked states do not increase the QBER per se, this attack can remain undetected,

thus enabling an intercept-resend attack. Nevertheless, they found a side effect that increased the QBER: the after-pulse generation as a consequence of the accumulated charge carriers in the detectors. The authors have also studied the conditions to make the after-gate attack feasible despite the side effect, and suggested countermeasures to avoid the attack. A summary of attacks targeting the photocurrent mode of gated InGaAs APDs is given in [Yuan et al., 2011b].

In [Lydersen et al., 2011a] it is demonstrated that an eavesdropper can threaten the security of certain QKD systems that use *superlinear threshold detectors*, if she carefully selects the amplitude of the trigger pulses. In addition, the authors show that APD-based gated detectors have a superlinear response at the falling edge of the gate. Therefore, they show that gated detectors could be attacked by using faint trigger pulses with less than 120 photons per pulse. They also emphasise that the ordinary security proofs are not applicable to systems using those detectors.

### Other attacks

If the receiver's equipment in a QKD implementation is fixed and does not depend on a choice of basis set for each qubit transmission, then the system is totally insecure against an eavesdropper that has access, even just once, to Bob's apparatus, as shown in [Boyer et al., 2012]. This paper presents a *fixed apparatus attack*, which is a special and very interesting case of the *reversed-space attack* proposed in [Gelles et al., 2012].

Another proposed attack against a two way plug-and-play QKD system is the *passive faraday mirror attack* presented in [Sun et al., 2011]. The Faraday Mirror (FM) plays a significant role in the stability of these systems by compensating the birefringence of the fibre. Nevertheless, practical FMs are imperfect, which causes the QBER to increase leaving a loophole for Eve to eavesdrop the key. Sun *et al.* show that under this attack the QBER induced by Eve is much lower than 25%, which is the QBER for the general intercept-resend attack when the FM is perfect. Indeed, if Eve implements a phase remapping attack against a system with an imperfect FM, the QBER introduced can be lower than 11%, which is the security threshold for the BB84 protocol under

the *collective attack* [Biham et al., 1997] and one-way post-processing. The authors also remark that, as the probability of Eve being successful depends on the loss of the channel, passive faraday mirror attacks are only viable in long-distance QKD systems.

#### 2.4.4 Device-Independent Quantum Cryptography

The above subsection stresses the advantages of making quantum cryptography potentially independent from the devices used in their implementation. Several works have intended to prove the security of QKD independently from the operating characteristics of the system, which is done by minimising the assumptions that must be made about the supposed “always ideal” behaviour of the hardware equipment employed in the experiments [Mayers et al., 1998], [Gottesman et al., 2004]. This is what *Device-Independent Quantum Key Distribution* (DIQKD) proposes [Acín et al., 2007]: a new form of cryptography that frees the security of the protocol from any assumptions on the internal working of the devices (which can even have been manipulated by an attacker), and aims to close the gap between the real implementations and the theoretical proposals of QC. DIQKD is possible through a protocol of quantum key distribution based on the observation of Bell’s inequality [Ekert, 1991], which guarantees that some amount of data is secure independently of how these data was generated. The security proof of the above mentioned DIQKD protocol is presented in detail in [Pironio et al., 2009].

Varizani and Vidick have recently proposed the first device-independent security proof of a QKD protocol, which guarantees the generation of a linear amount of the key even when the devices are subjected to a constant noise rate [Vazirani et al., 2012]. The only assumptions in this paper are that the stations of Alice and Bob are spatially isolated and that both, as well as Eve, are bound by the laws of quantum mechanics.

An experimental realization of DIQKD is still to be made although several proposals have already been made [Gisin et al., 2010]. An optical setup is necessary to test Bell’s inequality and this will have losses due to various factors, such as the coupling efficiency of the entangled pairs into the transmission line, transmission losses of the channel, absorption losses of the optical



components, etc. One has to assume that these losses could be used by an adversary in malicious ways. This is commonly referred to as the *detection loophole*. Thus, it has been established that in order to guarantee security, the detection efficiency, which takes into account the efficiencies of the transmission line and the single-photon detectors, should be in the order of 82.8%. This value is very strict and makes a realistic implementation an enormous challenge. One can assume that it will be facilitated when a quantum repeater becomes a reality, but until then an experimental demonstration faces serious difficulties.

In the case of devices being reused, a critical weakness of DIQKD protocols has been recently identified in [Barrett et al., 2012], where a *memory attack* is presented. It is based on the fact that some devices may store their inputs and outputs during one protocol run, and in the public discussion step of subsequent protocol runs they reveal some information about the recorded data. Possible countermeasures against this attack are quite impractical and include the destruction or the isolation of the devices after a single use.

As a resume it can be stated that the security of QKD is dependent upon the validity of the laws of quantum mechanics, and upon the assurance that no leakage of information takes place in the practical implementations. Very careful examinations of QKD systems are necessary for each application, and even then, no guarantee exists that the system will not be vulnerable. In fact, commercial QKD systems that have been sold over the past years as secure contained a serious vulnerability on them [Lydersen et al., 2010a], [Jain et al., 2011a]. An excellent review about the security of practical QKD, with essential theoretical tools that have been developed to assess the security of the main experimental platforms, can be found in [Scarani et al., 2009a].

## 2.5 Experimental free-space QKD systems

In this section a summary of the most representative experiments in the field of quantum communications over free-space links of several distances using different QKD protocols is presented.

The feasibility of free-space QKD systems relies on their capacity for transmitting and detecting single photons through the atmosphere in highly

challenging conditions of background radiation and turbulence of different magnitudes. Daytime operation is especially demanding due to solar background light, which increases the error rate if no careful filtering measures are taken.

One of the first practical free-space QKD experiment was reported in [Buttler et al., 1998a], where the authors developed and successfully tested a QKD system that implemented the B92 protocol over a free-space optical link of close to 1 km under nighttime conditions. The system was also tested over 240 m, demonstrating that QBERs of 0.7% or less could be achieved.

The viability of free-space QKD over kilometer-scale distances was later demonstrated in both daylight [Buttler et al., 2000] and at night [Rarity et al., 2001]. In [Hughes et al., 2002a] and [Hughes et al., 2002b] measurements were taken under both daylight and nighttime conditions in an experiment over a 10 km path. That same year, secure key exchange over a free-space link was achieved for an extended distance of 23.4 km between two mountains [Kurtsiefer et al., 2002]. The results of these free-space trials showed the possibility of implementing global quantum key exchange systems based on quantum communication satellites [Pfennigbauer et al., 2005]. Indeed, the first experimental analysis of the conditions needed for the implementation of the single-photon exchange between an Earth-based station and a satellite was reported in [Villoresi et al., 2008]. Also, the actual feasibility of satellite QKD with present technology has been analysed in [Bonato et al., 2009b], among other studies.

Experiments at much longer distances have been conducted, most notably the quantum communications experiments across a 144-km path in the Canary Islands (see [Ursin et al., 2007], [Schmitt-Manderbach et al., 2007], and [Fedrizzi et al., 2009]). These are the longest QKD experiments to date, which have achieved secure key generation over a free-space link at a rate of 12.8 bits/s [Schmitt-Manderbach et al., 2007]. This distance is considered sufficient to simulate the conditions of a satellite downlink [Meyer-Scott et al., 2011].

Using the above mentioned 144-km free-space link in the Canary Islands, three different configurations were established [Scheidl et al., 2009]. In the first one an entangled photon source was placed at Alice's location, resulting

in a quantum channel attenuation of 35 dB. In the second configuration the source was located asymmetrically between Alice and Bob, and the attenuation was 58 dB. Finally, when the source was symmetrically placed in the middle between Alice and Bob, the measured attenuation was 71 dB. Those attenuation proved that entanglement-based QKD systems can tolerate higher channel losses than systems based on weak coherent laser pulses, in particular when the source is located symmetrically between the two communicating parties [Ma et al., 2007], [Ma, 2008]. This confirmed that, when entangled-state sources are located symmetrically in the middle between Alice and Bob, QKD is feasible over distances of 300 km and even more.

Regarding systems that can operate at higher rates, in [Bienfang et al., 2004] the successful exchange of sifted keys over a 730-meter free-space link at transmission rates of up to 1 Mbps (sifted key rate) was demonstrated. A classical channel at a wavelength of 1550 nm for synchronisation purposes was sent in parallel with the quantum channel at  $\lambda \sim 845$  nm.

Other experiments have been conducted to implement and test different QKD systems in realistic atmospheric conditions. Several free-space QKD experiments using entangled photons were performed over horizontal distances from 0.7 km to 1.5 km [Erven et al., 2008a], [Erven et al., 2008b] and [Erven et al., 2010]. A complete experimental implementation of a free-space QKD system through a distance of 1.5 km using polarisation-entangled photon pairs from a compact parametric down-conversion source was reported in [Marcikic et al., 2006]. After error correction and privacy amplification average key generation rates of 630 bits/s were observed throughout ten hours of continuous communication. Apart from a classical wireless link, no specific hardware channel was required for synchronisation. The same distance of 1.5 km was demonstrated in a QKD study operating at a mid infrared wavelength to mitigate adverse foggy conditions [Temporao et al., 2008]. Other experiments related to long-distance polarisation-entanglement implementations are reported in [Aspelmeyer et al., 2003] and [Resch et al., 2005].

An experimental free-space QKD system using continuous variables was demonstrated in [Elser et al., 2009] and [Heim et al., 2010]. In these works a local oscillator was employed as spatial and spectral filter, which allowed daylight operation with no restrictions. The system used binary encoding on

coherent polarisation states and the quantum states were transmitted over a 100-m real atmospheric channel.

An entanglement-based free-space QKD system that links three buildings was described in [Weihs et al., 2007]. The entangled photon pair source was located on the rooftop of a building, which was located about 435 m from the building where Alice was housed. Bob’s location was about 1325 m from the source, the distance between Alice and Bob being about 1575 m. Single-mode optical fibre connected the source to two telescopes that transmitted the photons to Alice and Bob respectively. The authors pointed out that at the time of submitting the paper they had performed experiments that included only the 435-m link, while the second photon in each pair was detected locally at the source location. In this configuration total detected pair rates of up to 800 per second were obtained. This yielded a raw key rate of 400 bits/s, which depending on the QBER would produce a lower final key rate after error correction and privacy amplification.

Many free-space QKD implementations are limited to nighttime operation. In [Peloso et al., 2009] a lean entanglement-based QKD system was presented. It implemented spectral, spatial and temporal filtering techniques, which allowed continuous operation under varying light and weather conditions during several days. Key rates of 385 bits/s were reported, including error correction and privacy amplification processes. The reduction in the error rate due to daytime background photons that can be achieved by strong temporal filtering was also pointed out in [Restelli et al., 2010]. The reported free-space QKD system implemented temporal gating down to 50 ps. This was made by using fast-clock-recovery and commercial single-photon detectors modified with additional electronic circuitry to enhance timing resolution. Transmitting over 1.5 km and at clock rates of 1.25 GHz (800 ps between transmission events), the observed QBER during daytime was of 4%, which was less than one-third of the error rate obtained when no temporal gating was used.

A free-space QKD system developed in the context of the SECOQC Project at the University of Munich was described in [Peev et al., 2009]. It employed the BB84 protocol with decoy states using polarisation encoded attenuated laser pulses with a wavelength of 850 nm. Spatial filtering was used to reduce

the background light so that the system could operate during the day. Random sequences of WCPs of different polarisation and mean photon number were generated by using eight laser diodes. Two stations separated a distance of 80 m were connected at a high rate ( $> 10$  kbps) with a stable connectivity to the QKD network in a 24/7 operation regime. In [Benton et al., 2010] an autonomous system was also left running and generating shared key material continuously for over 7 days.

In addition to the above mentioned experiments along horizontal propagation paths of different distances, several other experiments have been conducted along ground-to-aircraft and ground-to-space communication paths [Toyoshima et al., 2008], [Villoresi et al., 2008], [Bonato et al., 2009a]. Since free-space QKD on earth has a distance limitation of a few hundred kilometers, immediate direct solution for global coverage is the use of earth-to-satellite links. Although the quantum channel in a satellite uplink may have very high transmission losses, in [Meyer-Scott et al., 2011] a system using weak coherent pulses and decoy states, which enables QKD operation with channel losses up to 57 dB, has been described. Recently, the first demonstration of key exchange with rapidly moving stations (QKD between an aeroplane and a ground station) has been reported [Nauerth et al., 2013].

Finally, [Tunick et al., 2010] presents interesting figures showing the quantitative relationships between the propagation distance or the transmission speed, and the year several free-space quantum communication experiments were performed, including a description of the different QKD protocols and photons source wavelengths used in them.



## Chapter 3

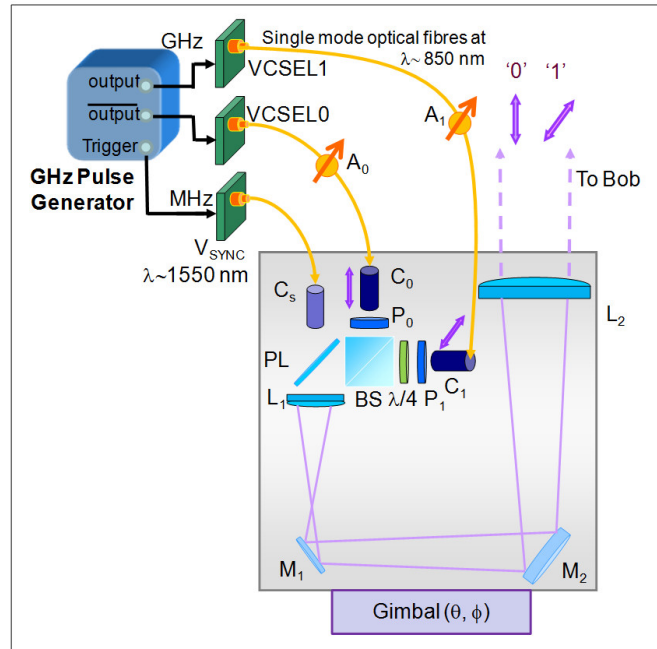
# Design and characterisation of the transmitter

A QKD system consists of three main parts: the transmitter, the transmission or also called *quantum* channel, and the receiver. The setup and experimental characterisation of the transmitter will be described in this chapter. Firstly, a general view of Alice setup will be provided, followed by several considerations regarding the design and performance of the emitter. Among such implementation forethoughts, the generation of the Alice's sequence will be first commented. Then, the choice of highly attenuated coherent light pulses as an approximation of single photons will be discussed. Subsequently, the characterisation of two vertical-cavity surface-emitting lasers, the selected light source, is described regarding mainly their driving conditions and spectral behaviour. Three essential points in the design of the transmitter will also be discussed: the linearity of the polarisation states encoding the '0's and '1's of the key, the timing synchronisation between emitter and receiver, and the alignment of Alice's three optical output

beams. Finally, the gimbal system where Alice is mounted on and the shielding from background radiation will also be described.

### 3.1 Setup of the transmitter

Figure 3.1 shows the layout of the transmitter. The purpose of the transmitter module—in the following often called “Alice module”—is to send out individual photons carrying binary information encrypted in two non-orthogonal linear polarisation states.



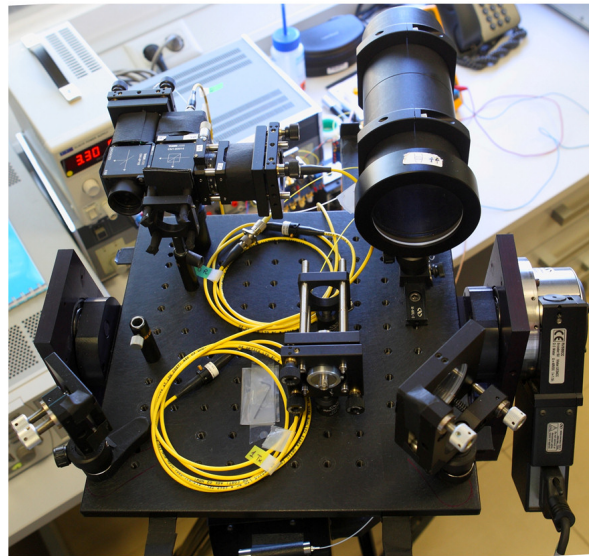
**Figure 3.1** – Diagram of the transmitter: Alice. VCSEL0 and VCSEL1 are two lasers emitting at  $\lambda \sim 850$  nm;  $V_{SYNC}$  is a third laser emitting at  $\lambda \sim 1550$  nm, which is used for the timing synchronisation and is combined with the  $\lambda \sim 850$  nm pulses by means of a broadband pellicle beam splitter (PL);  $A_0$  and  $A_1$  are two fibre-optic attenuators;  $C_0$ ,  $C_1$  and  $C_s$  are three collimators;  $P_0$  and  $P_1$  are two high extinction-ratio polarisers; BS is a non-polarising beamsplitter;  $L_1$  and  $L_2$  are two achromatic doublet lenses, which constitute the emitter’s telescope; and  $M_1$  and  $M_2$  are two high-reflectivity mirrors.

This is achieved by driving two laser diodes—one for each linear polarisation—with electrical pulses, and heavily attenuating the optical output



to an average photon number much below one photon per pulse. For that purpose Alice uses a fast GHz pulse pattern generator in conjunction with  $\lambda \sim 850$  nm *vertical-cavity surface-emitting lasers* (VCSELs) controlled by drivers that can operate at several Gbps. Each laser output is then sent to a fibre-coupled attenuator, which also spatially filters the beam ensuring that only one spatial mode is propagated. The attenuators are set so that Alice sends out pulses with a mean photon number per pulse of  $\mu \sim 0.1$ . Each attenuated signal is then coupled into a collimator and a high extinction-ratio polariser to produce the required linearly polarised quantum states. The states are then combined by a non-polarising beamsplitter cube.

The timing synchronisation between emitter and receiver is carried out by another beam at a different wavelength ( $\lambda \sim 1550$  nm), which conveys Alice's internal clock signal to Bob. The synchronisation beam is combined with the two polarisation states by using a broadband pellicle beamsplitter. The three combined beams are then collimated and expanded to a diameter of  $\sim 40$  mm by using a set of two achromatic doublet lenses. Finally, the transmitter is mounted on a high-precision gimbal system, which facilitates the alignment and pointing with the receiver. A picture of Alice module can be seen in Figure 3.2.



**Figure 3.2** – Picture of Alice module.

In the following sections, the main components of the transmitter unit and their characterisation will be described in detail.

### 3.2 Generation of Alice's sequence

The generation of Alice's sequence of electrical pulses that modulate the lasers is performed by an Agilent 81133A Pulse Pattern Generator (PPG) with low RMS jitter ( $< 1.5$  ps) and a large operating frequency range (15 MHz to 3.33 GHz). The PPG is capable of generating pseudo-random bit sequences (PRBS) from  $2^5 - 1$  to  $2^{31} - 1$  of bit length. Its two channel outputs, inverted and non-inverted, are used to drive both VCSELs (VCSEL0 and VCSEL1 in Figure 3.1) with non-return-to-zero (NRZ) signals. Thus, when one VCSEL is off the other one is on and vice versa. The trigger output is used to drive the synchronisation laser.

The Agilent 81133A PPG can be programmed through several remote programming interfaces [Agilent, 2007]. For remote controlling of the generator, the USB interface is used to establish the connection between a PC and the instrument. The LabVIEW environment is utilised to generate a pre-programmed sequence of a determined length, which by means of SCPI commands is set as the data pattern of the PPG. A short sequence is also inserted at the beginning of Alice's transmission to help correcting the temporal delay between Alice and Bob's sequences.

### 3.3 Source of single photons

Ideally, to emit the individual photons that encrypt each bit composing the secret key single-photon sources should be used. However, protocols using attenuated coherent states achieving equivalent security levels have been demonstrated [Lucamarini et al., 2009]. Moreover, though great efforts are being made in the field [Collins et al., 2010], current single-photon sources have still low efficiencies to enable high transmission rates [Gérard et al., 2004], [Bimberg et al., 2010], [Claudon et al., 2010], [Grangier, 2006]. In the system presented in this thesis the sender heavily attenuates a laser source, thus emitting the so called *weak coherent pulses* (WCP) that follow a Poisson distribution. For

that purpose two variable fibre-optic attenuators are used to provide a mean photon number per pulse of  $\mu \sim 0.1$ , which guarantees that only 0.5% of the emitted pulses contain more than one photon. Vertical-cavity surface-emitting lasers were used as laser source by the emitter and will be discussed in detail in the following subsections.

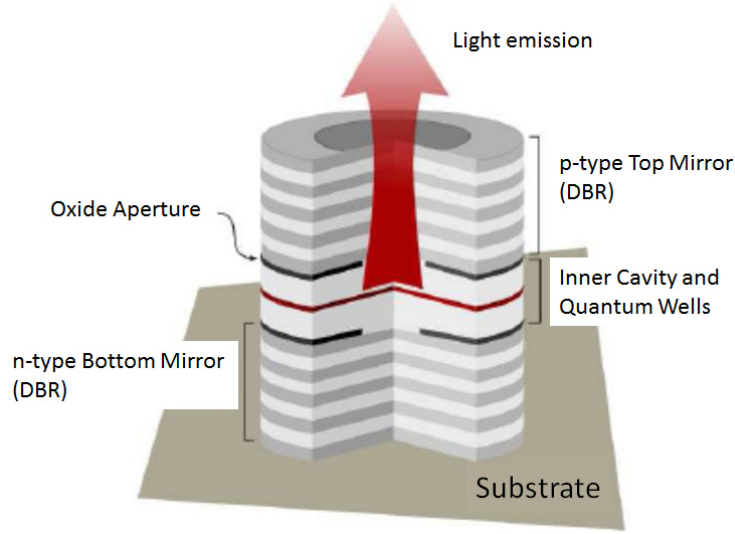
### 3.3.1 Vertical-cavity surface-emitting lasers

VCSELs controlled by high-speed drivers, which can operate up to 4.25 Gbps, were used at the emitter to achieve high transmission rates. A VCSEL is a semiconductor laser that emits the light perpendicularly to the active-layer plane. The optical cavities of VCSELs are very small, from one to three times the wavelength emitted. Therefore, the probability that a photon travelling through the cavity triggers the stimulated emission in a single pass is very low. This makes high reflectivity mirrors essential for VCSELs. High reflectivity mirrors are usually achieved by periodically alternating layers of different refractive indexes, as it can be seen in the schematic shown in Figure 3.3. Such structure is known as *Bragg reflector* [Smith et al., 2007, §17.4]. The Bragg condition provides the width the layers must have,  $\Lambda$ , for the reflected waves to be in phase:

$$2n_{eff}\Lambda = m\lambda , \quad (3.1)$$

$n_{eff}$  being the effective refractive index,  $m$  an integer and  $\lambda$  the wavelength of emission. A Distributed Bragg Reflector (DBR) is a structure formed by multiple layers of alternating materials such as GaAs and AlAs, each layer with a thickness of  $\lambda/4$ . High reflectivities of typically 99.5% can be achieved with a DBR [Hastings et al., 2005].

When *population inversion* is achieved, that is, when the injected carrier density is above a certain level in the active layer, the cavity exhibits optical gain. The minimum laser pump current needed for the optical gain to compensate for the losses in the cavity is called the *threshold current* [Agrawal, 2002, §3.3.2]. To minimise energy costs the threshold current should be as small as possible. The main advantages of VCSELs when compared to *edge-emitting lasers* [Agrawal, 2002, §3.4.4] are their small size, which allows them to be



**Figure 3.3** – Schematic gain structure of a VCSEL. The optical emission of a VCSEL is perpendicular to the active layer (after [DTU, 2012]).

grown in arrays [Uchiyama et al., 1985], [Jewell et al., 1991], their operation at low laser thresholds [Iga et al., 1987] and their low cost.

The operation spectral range of VCSELs based on GaAs technology includes wavelengths from  $\lambda \sim 650$  nm to  $\lambda \sim 1300$  nm. The VCSELs used for the QKD system investigated in this thesis were GaAs HFE4192-582 Finisar VCSELs designed for an emission wavelength of  $\lambda \sim 850$  nm and a maximum modulation rate of 4.25 Gbps.

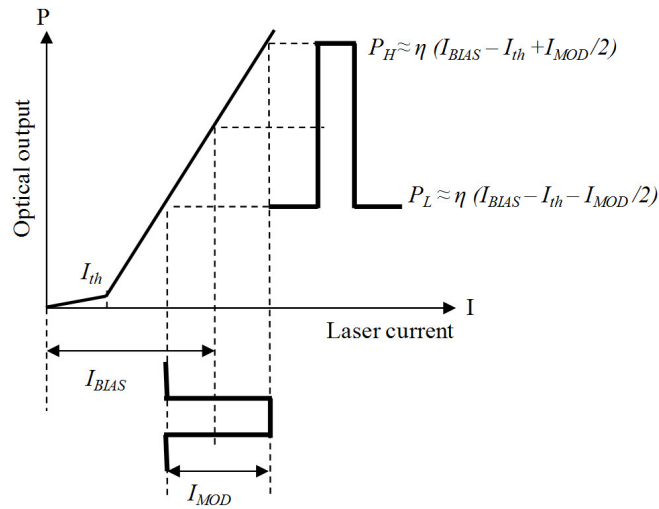
### 3.3.2 Wavelength choice

Two low-absorption atmospheric spectral windows in the near-infrared regions of  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm are usually considered for free-space optical communications. The latter wavelength has an associated higher transmission (see Figure 4.2, section 4.1.3) and it is slightly less affected by turbulence effects and backscattering. However, detection technology must also be considered. The advantage of choosing  $\lambda \sim 850$  nm relies mainly in the possibility of taking advantage of the more mature technology of Silicon-based single-photon detectors. Indeed, while InGaAs single-photon detectors have greatly improved their performance in terms of the maximum repetition rate they can

operate at (from MHz to GHz) [Yuan et al., 2008], they are still surpassed by commercially-available Si single-photon avalanche detectors (Si-SPADs) in critical parameters such as dark-count rate, detection efficiency and afterpulsing probability. Therefore, Si single-photon detectors permit the operation at higher repetition rates, which improves the key transmission rate. High transmission rates are essential in a future scenario where QKD might be used in conjunction with the Vernam cipher. Hence the importance of using laser sources and detectors that can operate at high frequencies. Therefore a source wavelength of  $\lambda \sim 850$  nm in conjunction with Si-SPADs as the single-photon detectors was chosen as the most efficient and practical solution to achieve GHz clock rates [Gordon et al., 2004].

### 3.3.3 Driver and circuit board interface

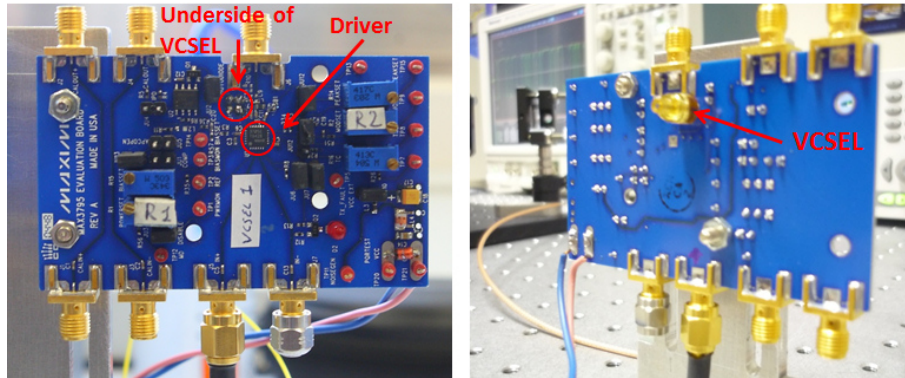
The primary function of a laser driver is to provide with suitable currents for bias and modulation of the laser diode (see Figure 3.4). The bias is a constant current that pushes the laser diode operating range beyond its threshold value and into the linear region. Modulation is an alternating current that is switched on and off in synchronisation with the input voltage waveform.



**Figure 3.4** – Input-output characteristics of the laser.  $I_{MOD}$  represents the modulation current,  $I_{BIAS}$  the bias current,  $I_{th}$  the threshold current,  $\eta$  is the slope efficiency, and  $P_L$  and  $P_H$  represent the low and high optical power levels, respectively.

The VCSELs were soldered onto two Maxim MAX3795 evaluation kits (EV kit). The MAX3795 EV kit consists of an electronic board, which provides complete optical and electrical evaluation of the MAX3795 VCSEL driver (see Figure 3.5). This driver contains a bias generator, a laser modulator and safety features. It also has an automatic power control (APC) that adjusts the laser bias current to maintain an average optical power output over temperature and changing laser properties. This is essential to perform quantum key distribution experiments, as the average photon number per pulse needs to be constant to typically 0.1, ensuring that the probability of two photons in the same laser pulse is as low as 0.5%.

The MAX3795 laser driver operates up to 4.25 Gbps. It introduces low jitter to the optical signal and is characterised by fast edge transitions, which combined with a high speed pulse pattern generator, enabled key distribution clocked up to 2.75 GHz, as will be discussed in chapter 6.



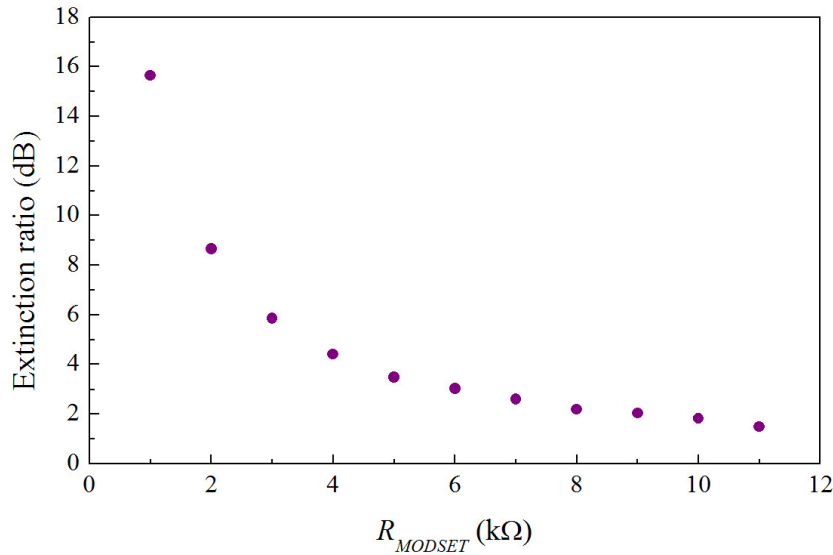
**Figure 3.5** – Photographs of the front (left) and back (right) of the MAX3795 driving board, where the HFE4192-582 Finisar VCSEL was soldered onto.

A variable resistor  $R_{MODSET}$  (R2 in Figure 3.5), located between the MODSET pin and ground, controls the modulation current out of the MAX3795 to the VCSEL. The bias current output of the MAX3795 is controlled by the resistor  $R_{BIASSET}$ , placed between the BIASSET pin and ground. In open-loop operation, BIASSET monitors the bias current level of the VCSEL. In closed-loop operation (when APC is activated),  $R_{BIASSET}$  limits the maximum allowed bias current, and the potentiometer  $R_{PWRSET}$  (R1 in Figure 3.5) is then used to adjust the desired average optical power output. The BIASMON

output provides a current proportional to the laser bias current, and it can be monitored at TP3 ( $V_{BIASMON}$ ) of the MAX3795 driver board using the equation below:

$$I_{BIAS} = \frac{9 \cdot V_{BIASMON}}{402} . \quad (3.2)$$

An optical evaluation of the signal emitted by the lasers was performed. The extinction ratio  $R_E$ , defined as the ratio of the high signal level to the low level, was evaluated at different modulation currents (i.e., different values of  $R_{MODSET}$ ) for a fixed bias current of  $\sim 9$  mA (see Figure 3.6). For that purpose, the optical output of each VCSEL was launched into a  $62.5 \mu\text{m}$ -diameter multimode fibre, which in turn was connected to a high-speed photodetector with a 2 GHz bandwidth and a responsivity of 0.4 A/W. The output of the photodetector was in turn connected to a 2.5 GHz bandwidth oscilloscope (model DPO 7254). The VCSELs were modulated with a square sequence at a frequency of 1 GHz. The extinction ratio in dB was then calculated as  $R_E(\text{dB}) = 20 \log(V_H/V_L)$ , where  $V_L$  and  $V_H$  are the low and high voltage levels of the signal displayed in the oscilloscope, respectively. Figure 3.6 shows that the extinction ratio increased with the modulation current (inversely proportional to  $R_{MODSET}$ ).



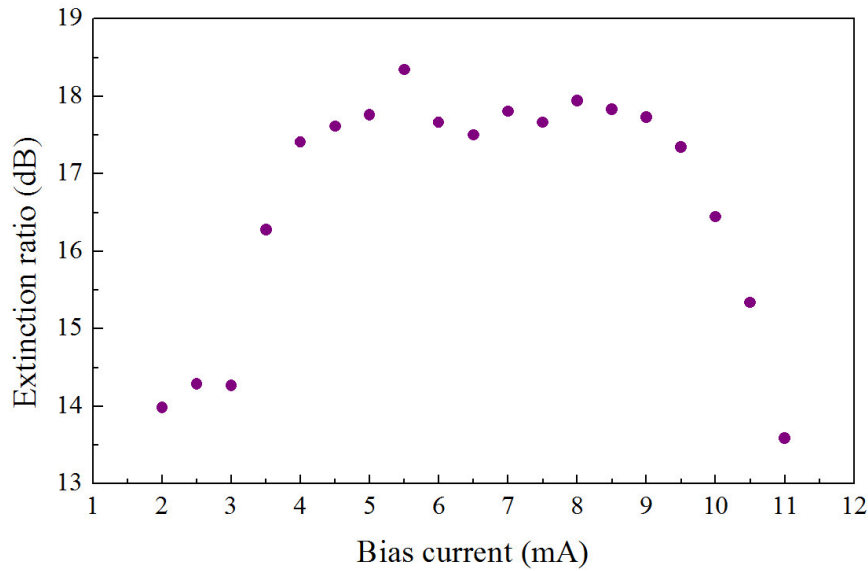
**Figure 3.6** – Extinction ratio of the optical output of VCSEL1 against  $R_{MODSET}$ , which is inversely proportional to the modulation current.



The extinction ratio can also be expressed as a function of the optical power levels as:

$$R_E(\text{dB}) = 10 \log_{10} \frac{P_H}{P_L} = 10 \log_{10} \frac{I_{BIAS} - I_{TH} + I_{MOD}/2}{I_{BIAS} - I_{TH} - I_{MOD}/2}, \quad (3.3)$$

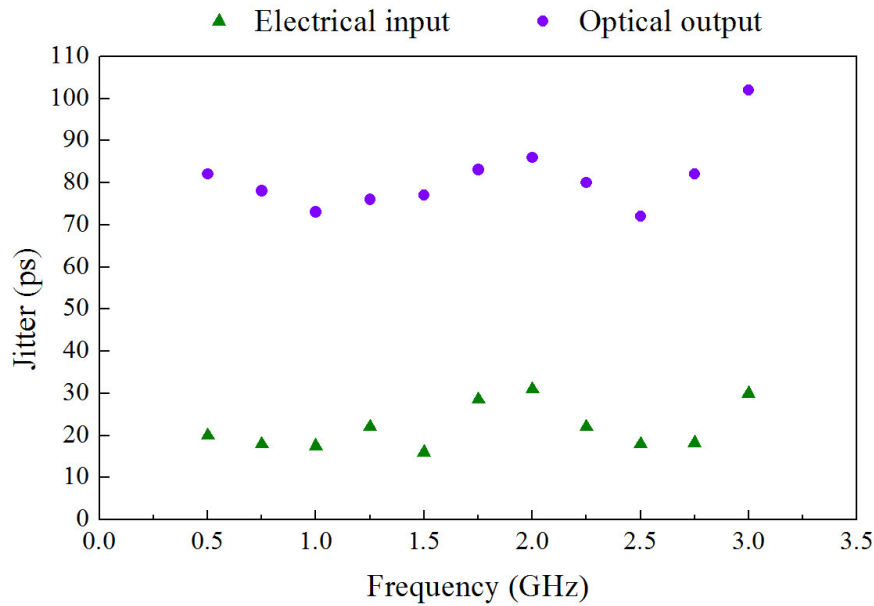
$I_{TH}$  being the threshold current,  $I_{BIAS}$  the bias current,  $I_{MOD}$  the modulation current, and  $P_L$  and  $P_H$  the low and high power levels respectively. It is obvious from Eq. 3.3 that high extinction ratios should be obtained for high values of  $I_{MOD}$ . The extinction ratio was also evaluated experimentally at different bias currents for the maximum modulation current. Figure 3.7 shows that the highest extinction ratios were measured for bias currents comprised between 4 and 9.5 mA. This interval of bias currents includes the theoretical optimum values, which for the typical values of  $I_{TH}$  (between 0.5 and 2 mA) and the maximum modulation current ( $\sim 15$  mA) were calculated from Eq. 3.3 to be between 8 and 9.5 mA. Although  $R_E$  is not exactly the same figure of merit as the QBER, it was still useful to estimate the optimal operation range for the modulation and bias currents of the VCSELs. Besides, the QBER program was still not developed at this point of the project.



**Figure 3.7** – Extinction ratio of VCSEL1 against the bias current for a maximum modulation current at 1 GHz clock frequency.



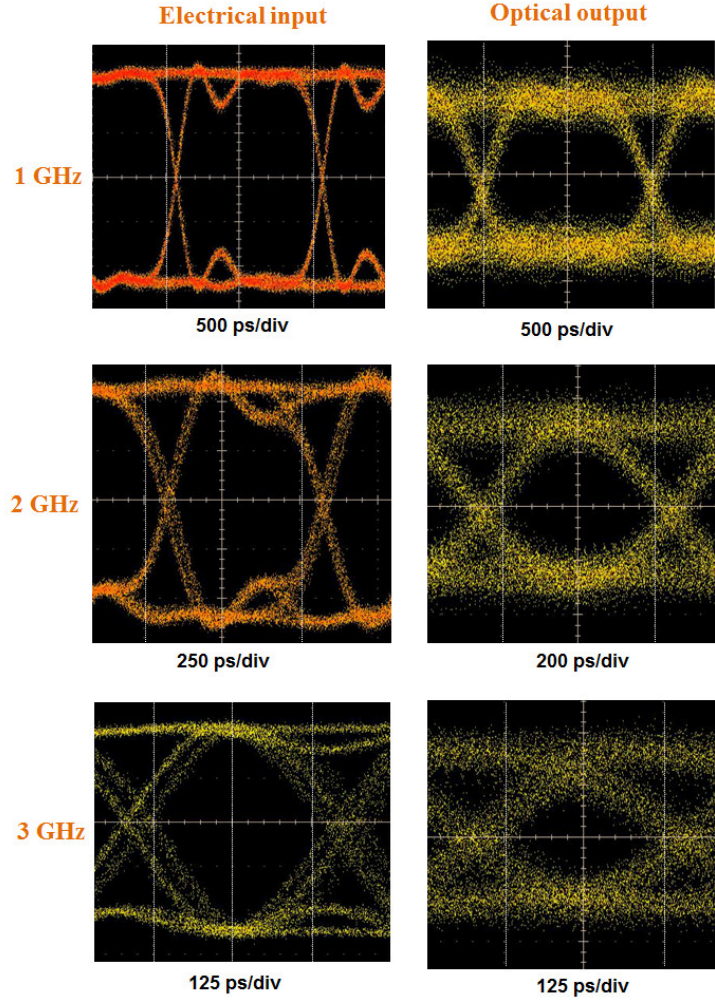
For a maximum modulation current and a fixed bias current the quality of the optical output emitted by the VCSELs was evaluated and compared with the electrical driving input. The jitter (peak-to-peak) was measured at different clock frequencies for a  $2^{31} - 1$  bits sequence. The photodetector and the digital DPO 7254 oscilloscope were used for that purpose. Figure 3.8 shows the measured jitter and Figure 3.9 the eye diagrams of the electrical and optical signals at clock frequencies ranging between 1 and 3 GHz.



**Figure 3.8** – Jitter of the electrical input of the MAX3795 driver and the optical output of the VCSEL0 against clock frequency.

Considering that the photodetector and the oscilloscope bandwidths are 2 GHz and 2.5 GHz respectively, the jitter of the optical signal was even lower than  $\sim 80$  ps at frequencies up to 2.75 GHz. At 1 GHz and 2 GHz some ringing effects were observed in the eye diagrams of the electrical signal. Moreover some reflections due possibly to impedance discontinuities in the circuit board were observed at 2 GHz and 3 GHz of the electrical eye diagrams. At 3 GHz some portions of the electrical eye diagram separate into two distinct lines. This is called Pattern Dependent Jitter (PDJ), which results from wide variations in the number of consecutive bits contained in NRZ data streams working against the available bandwidth. One condition that could cause this effect was an excessive modulation current that saturated the transistor, limiting its

high-speed switching capabilities. The decreased switching speed limits the bandwidth during the rising edge.

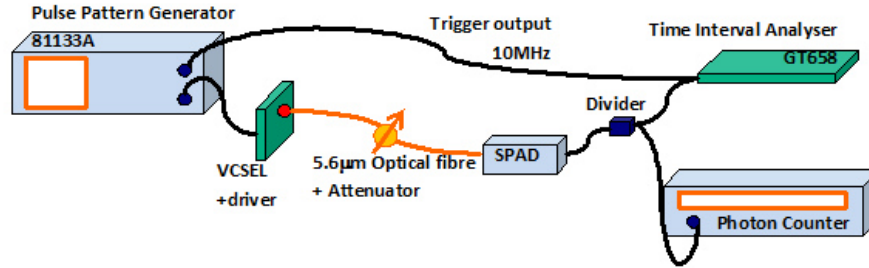


**Figure 3.9** – Eye diagrams of the electrical input of the laser driver and the optical output emitted by VCSEL0 at three clock frequencies.

### 3.3.4 Optimisation of the driving conditions of the VCSELs

In the previous section, the optimisation of the driving conditions of the VCSELs as a function of the extinction ratio of the emitted optical signal was described. This gives an approximate idea of the optimal driving conditions of the VCSELs but it is not as accurate as the information provided by

the QBER, which is the final parameter that needs to be optimised. For this purpose the setup shown in Figure 3.10 was used.

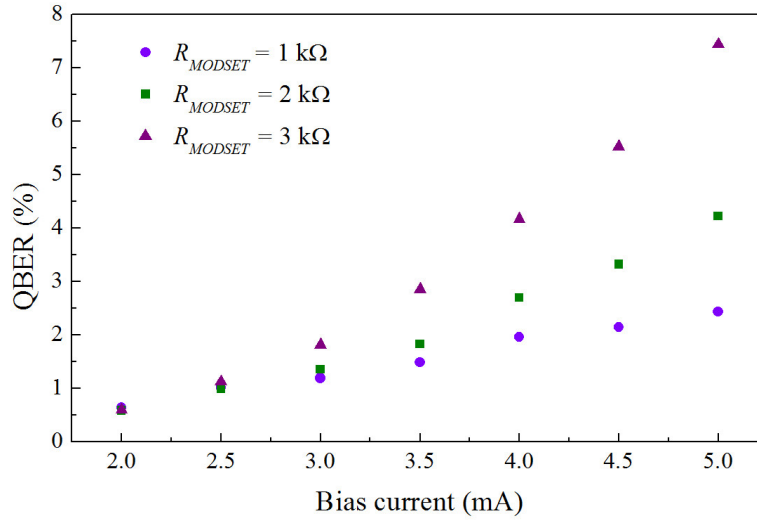


**Figure 3.10** – Schematic of the experimental setup for the optimisation of the driving conditions of the VCSELs.

The laser driving board was connected to a pulse pattern generator (PPG), which provided the electrical signal that drove the VCSEL. The laser output was then connected to a fibre-optic attenuator to approximately simulate the channel loss and the receiver efficiency of the QKD system. The output of the attenuator was connected to a Si-SPAD, the output of which was divided to monitor the count rate in a photon counter, and to record each photon arrival time with a Time Interval Analyser (TIA) card (discussed in section 5.4). These arrival times served to reconstruct the detected signal, which was then compared with the bit pattern used to modulate the laser in order to calculate the QBER or error rate, defined by the ratio of incorrect counts (those for which the detected bit value was different from the emitted bit) to the total number of detected events or number of photon arrivals. The trigger output of the PPG was set to 10 MHz and was directly connected to the external-clock input of the TIA to synchronise the transmitted and detected signals. The measured error rate in this experiment only takes into account the error rate due to the source of photons and the detectors of the QKD system, isolating it from the error rate contribution of all the optical components of the QKD system.

The bias and the modulation currents of the VCSEL were adjusted to find the minimum QBER. First, since it was previously established that high modulation currents provided high extinction ratios, three fixed values of the modulation current close to its maximum were chosen. For each of them, the

bias current was varied between 2 mA and 5 mA and the QBER was measured, as shown in Figure 3.11 (values taken for VCSEL0 at a clock frequency of 1 GHz). The same measurements were repeated for VCSEL1 obtaining similar curves. The optimal value, i.e., the lowest QBER, was obtained for a bias current of 2 mA for both lasers (the minimum bias current that could be set). This is due to the falling edge of the optical pulses not being abrupt, i.e., having an associated ‘tail’. This tail is then detected in the adjacent bit period, resulting in incorrect photon events that increase the QBER. Decreasing the bias current pushes down the high level of the optical signal, thus decreasing the length of these tails, and hence the QBER.

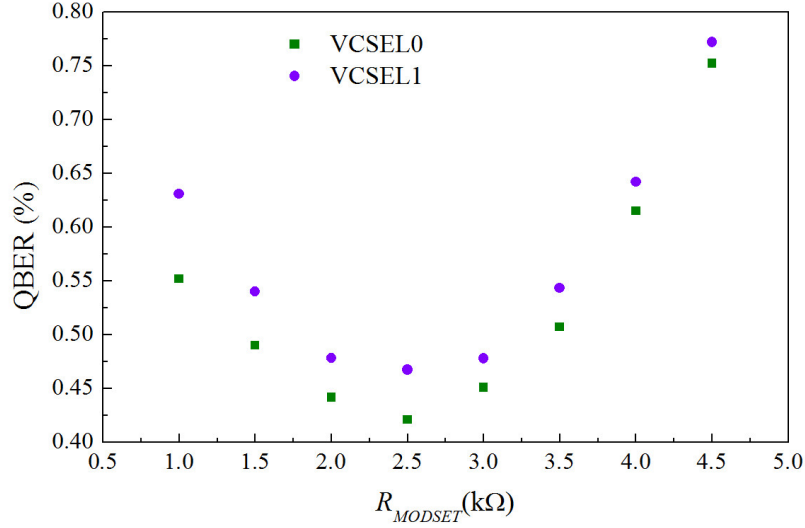


**Figure 3.11** – Quantum bit error rate against the bias current of VCSEL0 at three particular values of the modulation current and 1 GHz clock frequency.

Once established the optimal bias current (2 mA), the error rate was measured to determine the optimal modulation current (controlled by  $R_{MODSET}$ ), which from Figure 3.12 can be seen that corresponded for both VCSELs to a value of  $R_{MODSET}$  of 2.5 k $\Omega$  ( $\sim 6$  mA).

In the system under study, when one VCSEL is off the other one is on and vice versa. Therefore the off state plays a critical role in the QBER, since all photons detected in this level are counted as wrong events. Hence, it is essential that the off state of each laser emission be as close to zero as possible. Increasing the modulation current pushes down the off state of the optical

signal ( $P_L$  in Figure 3.4), which as just discussed decreases the QBER. The fact that the maximum modulation current (minimum  $R_{MODSET}$  in Figure 3.12) does not give the minimum QBER is likely due to relaxation oscillations that take place when the lasers are switched on from the completely off state.



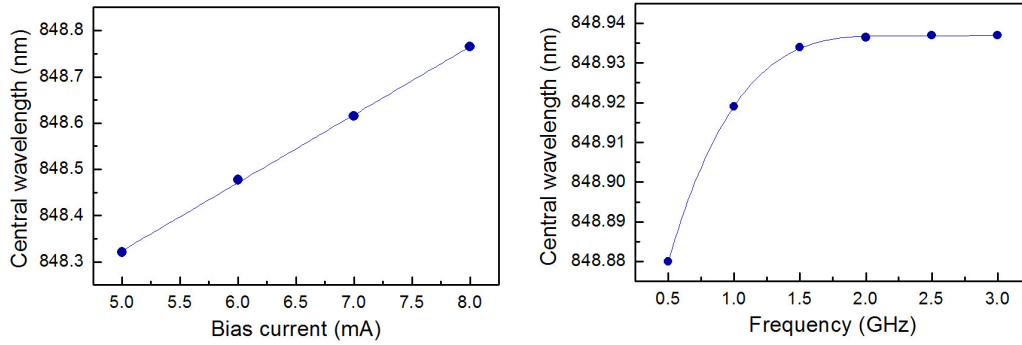
**Figure 3.12** – Quantum bit error rate against  $R_{MODSET}$  for both VCSEL0 and VCSEL1 at the optimum bias current of 2 mA and 1 GHz clock frequency.

### 3.3.5 Spectral analysis

The spectral behaviour of both lasers, VCSEL0 and VCSEL1, was characterised with an optical spectral analyser (OSA) ADVANTEST Q8384 as a function of several parameters: bias and modulation currents of the lasers, clock frequency and time. For simplicity purposes only the results obtained for VCSEL0 are represented in the following figures, but similar spectra and conclusions were drawn for VCSEL1.

To evaluate the influence of the bias current in the spectral characteristics of the VCSELs, the spectra of the lasers were taken as a function of the bias current for a fixed (optimal) modulation current. It was observed that when increasing the bias current the spectrum shifted towards higher wavelengths with a shift of  $\sim 0.15$  nm/mA, as shown in Figure 3.13 (left).

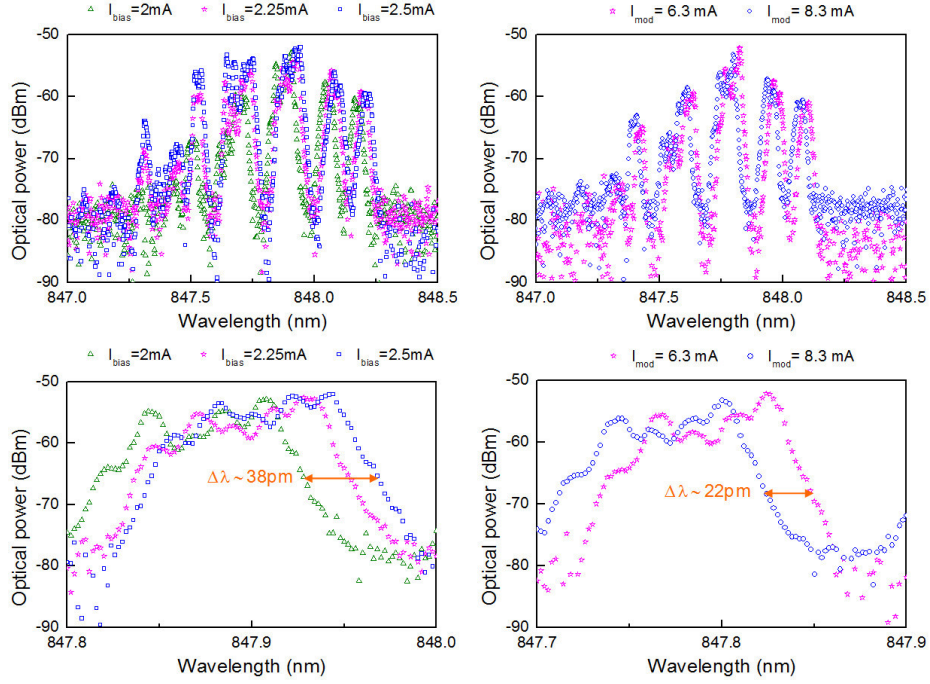
The dependence of the spectra with the clock frequency was evaluated for fixed values of the bias and modulation currents, and it is represented in Figure 3.13 (right), from which it can be concluded that the spectrum hardly shifted (60 pm) in the frequency range from 0.5 GHz to 3 GHz.



**Figure 3.13** – Central emission wavelength of VCSEL0 against the bias current (left) and against the clock frequency (right).

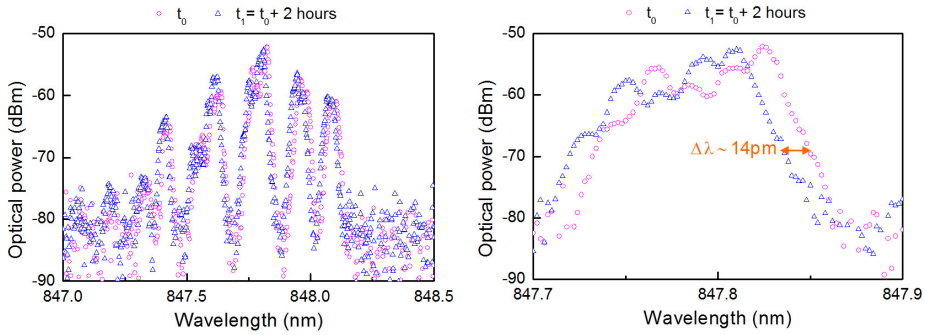
To characterise the spectral behaviour in the proximities of the optimum values of bias and modulation currents the spectral shift with bias at a fixed modulation current was represented in Figure 3.14 (top left and zoom in bottom left), and with modulation at a fixed bias in Figure 3.14 (top right and zoom in bottom right).

Figure 3.14 (bottom left) shows that for VCSEL0 a spectral shift of 38 pm can be observed for an increment of 0.5 mA in the bias current, i.e., the variation in bias current caused a shift in the central wavelength peak of VCSEL0 of 76 pm/mA, in the range of bias currents close to the minimum bias. Similarly, in Figure 3.14 (bottom right) a shift of the peak emission of 22 pm can be observed, corresponding to a variation of the modulation current of 2 mA, which means that the spectra only changed by approximately 11 pm/mA of modulation current. These changes with bias and modulation currents were considerably small. Nevertheless, since the bias and modulation currents for both VCSELs were set to fixed values (the optimum ones) through the measurements taken for the QKD system, the expected spectra variation was minimal.



**Figure 3.14** – Emission spectra of VCSEL0 at three different bias currents (top left) and zoom on the graph showing the spectral shift (bottom left); and emission spectra of VCSEL0 at two modulation currents (top right) and zoom (bottom right).

The spectral behaviour was also characterised with time and it was found that after two hours the spectrum only shifted 14 pm, as shown in Figure 3.15.



**Figure 3.15** – Spectra of VCSEL0 in two different instants (left) and zoom of the spectra showing a shift of 14 pm (right).

The APC of each VCSEL driver maintained an average optical power output over temperature and changes in laser properties. However, this is not



sufficient to guarantee complete indistinguishability of both VCSELs. This could be achieved by using a Peltier cooler in each VCSEL, which would fine tune their emission wavelength to a precise desired wavelength that would be identical for both. Moreover, since both VCSELs are multimode, a narrow bandpass filter would ensure that only one spectral mode propagates. However, due to the difficulty of attaching a Peltier cooler to the VCSELs since they were soldered onto an electronic board, this option had to be abandoned.

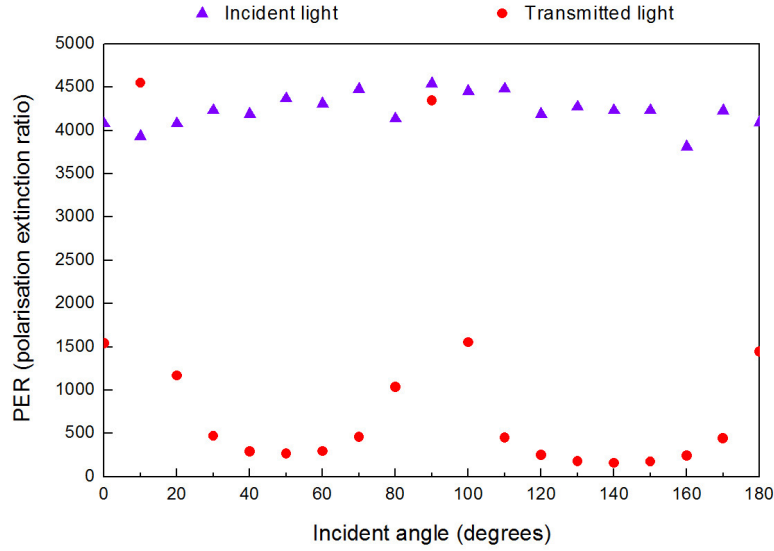
### 3.4 Characterisation of the polarisation states

Birefringence and polarisation dependent loss of optical fibres may modify the angle and linearity of the polarisation states. To prevent these undesirable effects Alice module was designed avoiding optical fibre once the polarisation states were defined. For this reason optical fibres were used in the emitter only to convey the photons from the lasers outputs to the collimators of Alice module. Therefore no birefringence due to optical fibres was introduced in the QKD system since only free-space optical components were employed in the transmitter and receiver optical modules (see Figure 3.1 and Figure 5.2).

The polarisation of the non-orthogonal quantum states should be maintained as linear as possible to minimise the QBER contribution due to photons detected in Bob with the wrong polarisation (*polarisation leakage*, see section 6.4). For this reason a thorough analysis of the *polarisation extinction ratio* (PER) through the optical components that could alter the polarisation of the quantum states was performed. The linearity of the diagonal state was particularly difficult to be maintained since it became elliptical due to several factors. Firstly, in the cube beamsplitter at Alice the junction of the two prisms at the cube has a lower refractive index than that of the material surrounding it, i.e., the incident medium is denser. Therefore, the situation of internal reflection is given ( $n_i > n_t$ ). In this case, for an incident angle  $\theta_i$  larger than the critic angle  $\theta_c$ , the phase difference  $\Delta\varphi$  between the two components of the electric field, parallel and perpendicular to the incident plane, is different from 0 or  $\pi$ , which means the incident linear state will acquire some ellipticity [Hecht, 2002, §4.6]. Moreover, in a more general case the material at the junction of the beamsplitter cube might have some absorption (the



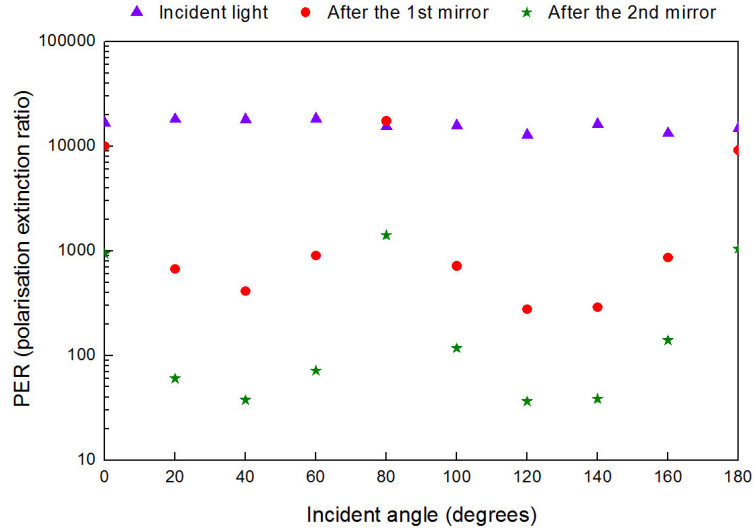
refractive index is complex). This means that  $\Delta\varphi$  of the polarisation states after passing through the beamsplitter is 0 or  $\pi$  (no change in ellipticity) only for incident angles of  $0^\circ$  or  $90^\circ$ . This can be observed in Figure 3.16, which shows the PER of the beam transmitted through the cube beamsplitter as a function of the incident angle of polarisation. The initial linearity of the polarisation states before passing through the beamsplitter is only maintained for incident angles of  $0^\circ$  or  $90^\circ$  ( $10^\circ$  and  $90^\circ$  in Figure 3.16, maybe due to imperfections in the measurement or in the beamsplitter). For the remaining angles the PER dropped significantly (from more than 4000:1 to less than 500:1).



**Figure 3.16** – PER of linearly polarised light incident on the cube beamsplitter and PER of the light after being transmitted through, against the angle of incidence.

This effect has also been studied for the light hitting the mirrors that are used to direct the beams in Alice module. Figure 3.17 represents the PER of the light reflected by the first mirror and after the second mirror as a function of the incident polarisation angle. The PER values show that the mirrors turn the incident linearly polarised beam into elliptical, except for the two mentioned angles of incidence where the absorption effect is minimum.

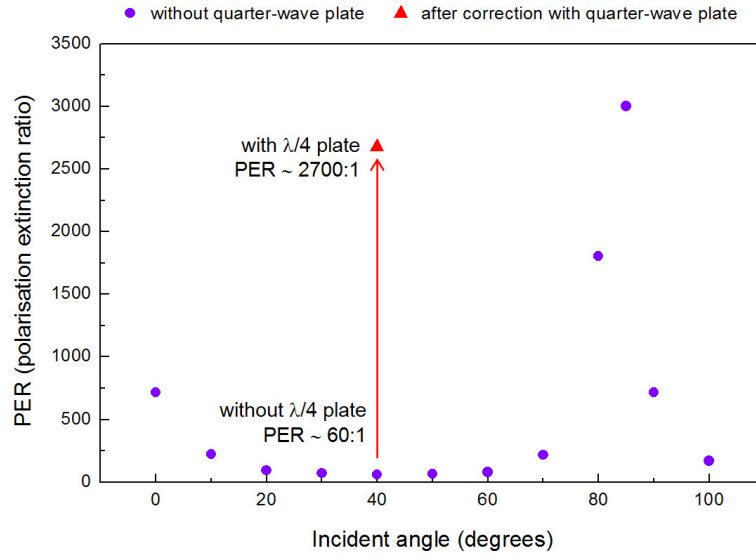
Since for one of the incident angles the PER still maintains high (for example for the angle of incidence of  $80^\circ$  in Figure 3.17), this incidence could be chosen as one of the two polarisation states necessary for the B92 protocol,



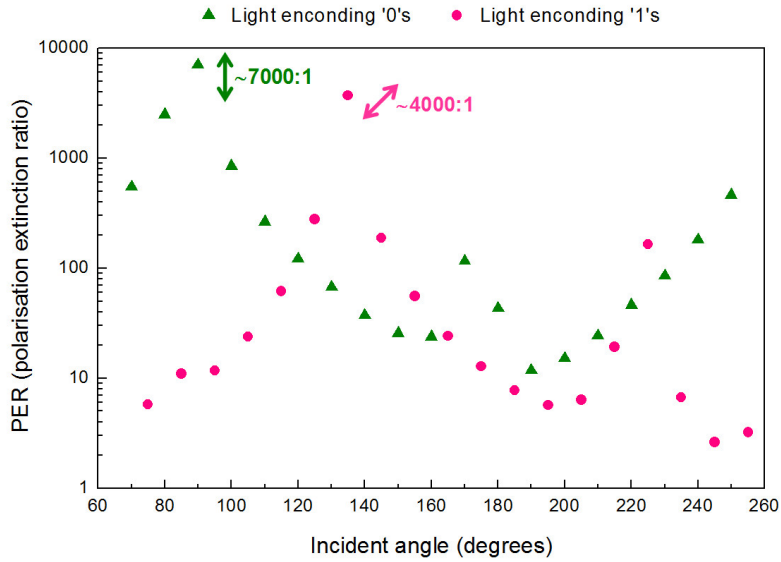
**Figure 3.17** – PER of linearly polarised light incident on the first mirror in Alice, reflected by the first mirror, and after the second mirror, as a function of the angle of incidence.

in this case the vertical state, which was set at  $P_0$  (see Figure 3.1). The other state, the diagonal one, had to be set at  $45^\circ$  from the vertical state and the low PER found at this angle made necessary some polarisation correction technique. For this effect a quarter-wave plate was placed between the polariser of the diagonal channel and the cube beamsplitter. The orientation angle of the quarter-wave plate was carefully optimised to compensate for the phase shift the components of the electrical field would suffer after passing through Alice. Figure 3.18 represents the PER of the light exiting Alice (transmitted through the cube beamsplitter, and reflected by the pellicle beamsplitter and the mirrors), as a function of the angle of polarisation set in  $P_1$  without correcting with the quarter-wave plate (circles) and after placing the quarter-wave plate to enhance the PER of the diagonal state (triangle). An improvement from 60:1 to 2700:1 after compensating the phase shift with the quarter-wave plate was observed.

Finally, Figure 3.19 shows the polarisation extinction ratio exiting Alice of the light emitted by VCSEL0 and VCSEL1 for different incident angles of polarisation (set in  $P_0$  and  $P_1$  respectively). The graph also shows the chosen angles of polarisation for the non-orthogonal quantum states encoding the ‘1’s and the ‘0’s of the transmitted sequence.



**Figure 3.18** – Polarisation extinction ratio of the light exiting Alice (from the transmission channel at the beamsplitter) against the angle of polarisation set in  $P_1$ ; without any polarisation correction (circles) and after correcting the diagonal polarisation state with a quarter-wave plate (triangle).



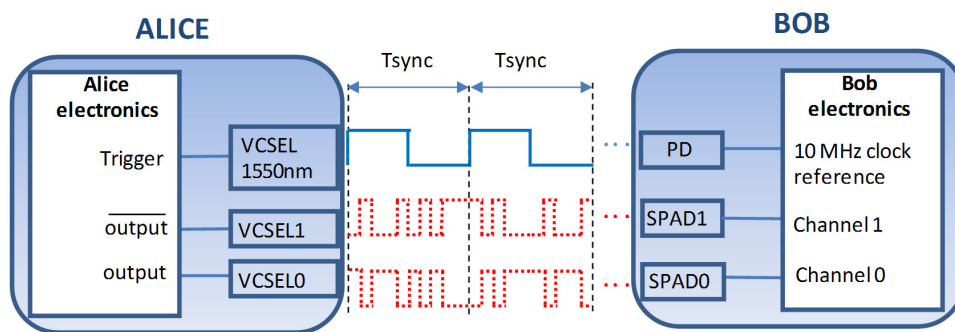
**Figure 3.19** – Polarisation extinction ratio of the quantum states at Alice's output against the incident angle of polarisation.

As the polarisation states need to be set at a relative angle of  $45^\circ$  for the implementation of the B92 protocol, the quarter-wave plate orientation was

adjusted to optimise the extinction ratio of the state at  $45^\circ$  (the diagonal state) from the state with the maximum PER (the vertical state). After that, a PER of  $\sim 4000 : 1$  was achieved for the diagonal state. The vertical state had a PER of  $\sim 7000 : 1$  and did not need any compensation.

### 3.5 Optical synchronisation

To synchronise emitter and receiver Alice sends out a periodic bright pulse of different wavelength from that used for the key at a sub-multiple value of the clock frequency. Figure 3.20 depicts a schematic of the synchronisation process. The wavelength chosen for that purpose was  $\lambda \sim 1550$  nm, since it transmits well in the atmosphere and off-the shelf components are available at this wavelength. It is also spectrally far from  $\lambda \sim 850$  nm, and therefore they can be easily discriminated in the receiver module using a dichroic mirror. The laser requirements were: to be fibre-coupled, since it reduced considerably the complexity of the setup and more importantly, to have a high bandwidth, so that the rise and fall times were sufficiently small and the jitter as low as possible not to increase the error rate of the system. The laser used was a RayCan 1550 nm single-mode VCSEL with single-mode fibre pigtail, capable of data rates up to 4 Gbps, with rise and fall times of typically 90–120 ps.



**Figure 3.20** – Schematic of the synchronisation process. Alice sends out a periodic bright pulse at  $\lambda \sim 1550$  nm synchronous with the signal carrying the key. The synchronisation signal is detected at the receiver side by an amplified photodetector (PD) and serves as the reference clock for the timestamp card in Bob.

The value of the synchronisation frequency was determined by the timestamp module in the receiver side, which has an external-clock input for a user supplied 10 MHz reference that has to be synchronous with the signal carrying the key. The synchronisation frequency at the emitter was obtained from the trigger output of the pulse pattern generator in Alice by subdividing the clock frequency so that the resulting frequency was 10 MHz. Therefore the trigger output served as the driving signal for the  $\lambda \sim 1550$  nm laser, which was soldered on a driver board identical to the board for the  $\lambda \sim 850$  nm VCSELs discussed in section 3.3.3.

In the transmitter module the  $\lambda \sim 1550$  nm VCSEL was connected to a collimator via a pigtailed single-mode fibre. The collimated beam was then combined with the  $\lambda \sim 850$  nm photons by means of a broadband pellicle beamsplitter, to be then expanded and sent to the receiver by the telescope composed by the set of lenses  $L_1$  and  $L_2$ , as depicted in Figure 3.1.

Although the lenses in Alice were achromatic, the spectral range did not cover the whole  $\lambda \sim 850$  nm to  $\lambda \sim 1550$  nm and hence there was some chromatic aberration. Therefore, as the telescope in Alice was adjusted to collimate the  $\lambda \sim 850$  nm beams, the  $\lambda \sim 1550$  nm beam diverged. This incurred in additional loss for the synchronisation signal, since it reached the receiver telescope larger than its optimal dimensions. However, this loss did not constitute a major problem, even for the experiments at 300 m, as the power in the receiver end satisfied the voltage requirements of the timestamp card, as it will be discussed in section 5.7.

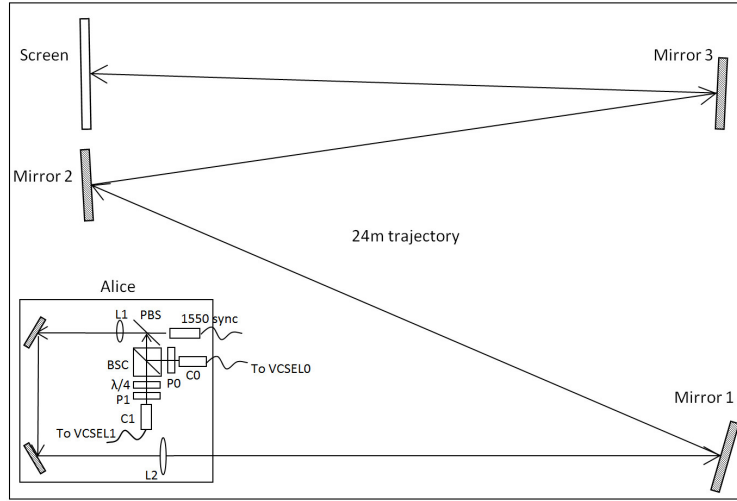
## 3.6 Beams alignment

The three laser beams in Alice, the two at  $\lambda \sim 850$  nm carrying the key and the synchronisation beam at  $\lambda \sim 1550$  nm, had to be made coincident in the far field since only one output telescope was to be used to expand and send the beams to the receiver. This coincidence of the beams was extremely important and had to be sufficiently precise for both  $\lambda \sim 850$  nm beams (encoding the ‘ones’ and the ‘zeros’ of the key) to be detected in the receiver end with the same efficiency.

Such a task was far from trivial with the original components of the transmitter module. The configuration of the initial version of Alice contained a gimbal mount for the beamsplitter cube (BSC), metrics of which was different from the metrics of the rest of mounts (for the polarisers, the collimators and the pellicle beamsplitter). Therefore, to adapt both types of metrics three custom-made aluminium sheets were used, two sheets for the coupling with the  $\lambda \sim 850$  nm channels and another sheet for the junction between the BSC and the pellicle beamsplitter (PBS). However it resulted impossible to make coincident the  $\lambda \sim 850$  nm beam transmitted through the cube with the other  $\lambda \sim 850$  nm beam reflected by the cube, and these in turn with the synchronisation beam, since due to the lack of sufficient accuracy in the fabrication of the aluminium sheets, the beams were from its origin at a slightly different height.

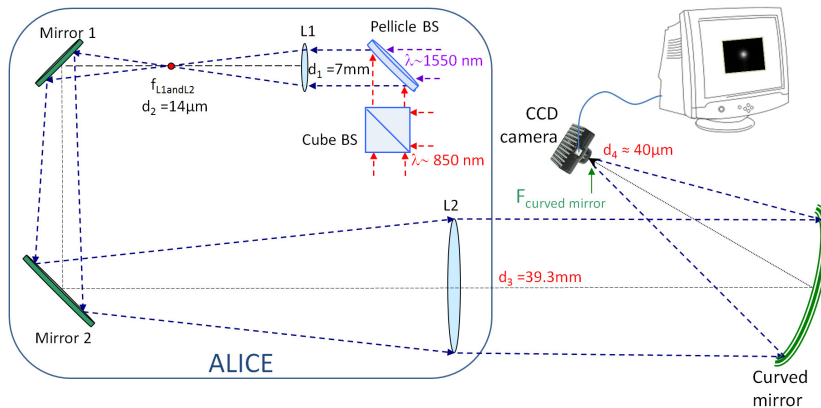
Consequently the gimbal mount for the BSC was replaced with a static mount of the same metrics as the other mounts. The gimbal mount of the original version of Alice provided with azimuth, elevation and rotation movements for the BSC, which in conjunction with the  $x-y$  mounts that were used to hold the collimators were useful to direct the beams with the aim to make them coincident. With the static mount however, these movements had to be achieved independently for each channel. Several combinations of three different types of mounts were tried to hold collimators: static,  $x-y$  and kinematic mounts. The size of each type of mount also played a role, since a compact design of Alice was desired. The coincidence of the three beams could finally be achieved with a static mount for the channel of the ‘0’s (which would be the reference beam), and two kinematic mounts, one for the synchronisation channel and other for the channel emitting the ‘1’s.

Figure 3.21 represents a schematic of the alignment technique. Three flat mirrors were utilised to extend the trajectory of the beams to  $\sim 24$  meters. The  $\lambda \sim 850$  nm beam that comes from VCSEL0 and gets reflected by the BSC—which we shall call the ‘0’ beam—was chosen as the reference beam for the alignment. Then the ‘1’ beam and the ‘sync’ beam were directed to the same point through each mirror, so that they kept coincident along the whole beam trajectory.



**Figure 3.21** – Method for the alignment of the three beams exiting Alice: ‘0’ beam, ‘1’ beam and ‘sync’ beam. The ‘0’ beam was the reference, whereas ‘1’ and ‘sync’ beams were aligned to the reference with the help of kinematic mounts.

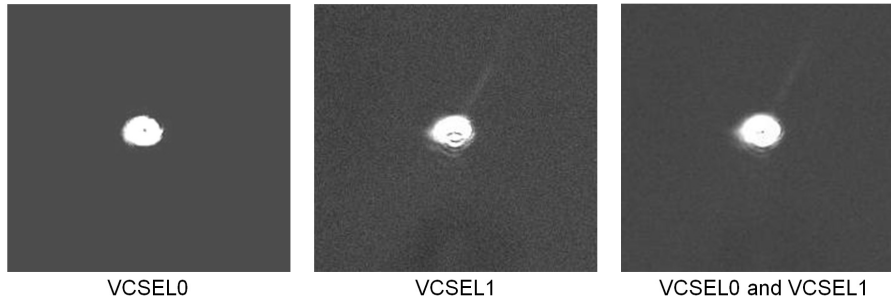
Next, a further technique for beam alignment was used to confirm the coincidence of the beams in the far field (see Figure 3.22). It consisted of the use of a curved mirror and a CCD camera placed at the focal length of the mirror. Parallel beams focus at the same point and coincident beams remain together when moving the CCD camera along the focus and Rayleigh zone.



**Figure 3.22** – Method for making the three beams from Alice coincident by using a curved mirror and a CCD camera.

A slight deviation between the ‘0’ and ‘1’ beams was observed. The ‘1’ (transmitted) beam was then directed to the exact position of the ‘0’ (reflected)

spot. Finally it was verified that the spots on the camera kept coincident along the optical axis of the curved mirror. Figure 3.23 shows the images of the beams at  $\lambda \sim 850$  nm on the CCD camera. The image centroids were calculated and their value proved that the positions of the spots on the CCD camera were the same.



**Figure 3.23** – Pictures taken by the CCD camera of the ‘1’ and ‘0’ spots, showing that they were coincident.

### 3.7 Gimbal system

All Alice’s optics is mounted on a 30 cm-side square optical breadboard, which is in turn mounted on a custom-made gimbal system that is used for the alignment of emitter and receiver. The gimbal scheme is shown in Figure 3.24.

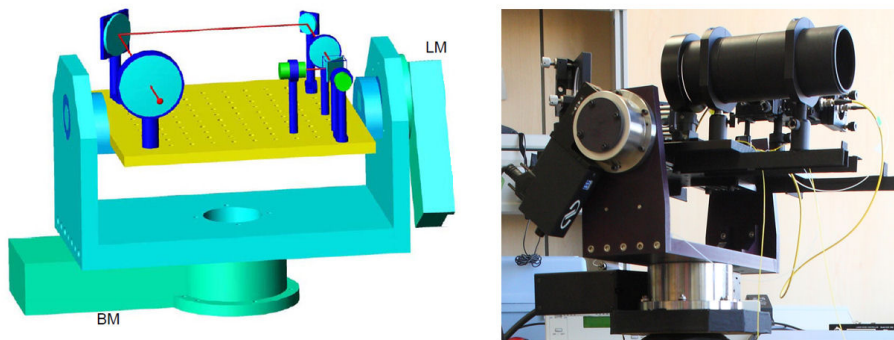
It consists of a structure that provides with the azimuth and elevation movements. Two rotation stages with high-precision angular positioning accuracy are employed for that purpose. Both are controlled by a programmable double-axis driver. The motor in the base supplies the azimuth trajectory and has a minimum incremental motion of  $0.001^\circ$ , while the lateral motor with a minimum incremental motion of  $0.00025^\circ$  provides the elevation rotation. In each lateral support of the gimbal structure a bearing holds a rod with an L-shaped holder where Alice is mounted on. Finally, the whole gimbal system is supported by a robust tripod, designed to bear a weight of up to 90 kg (see Figure 3.25).



### 3.8 Shielding the emitter from background radiation

The current design of Alice module reflects stray background light mainly through the mirrors, being partially sent out to Bob's telescope, thus increasing the error rate. Other setups of the transmitter optics are being considered so that mirrors become dispensable. However, an effective measure to reduce the amount of stray light that is coupled in the transmitter is the use of a blackout-material shield and a long tube around the main lens. Therefore a long antireflective tube was attached to Alice's main objective lens, and the whole module was also covered with a box built with light blackout cardboard and fabric (see Figure 3.26).

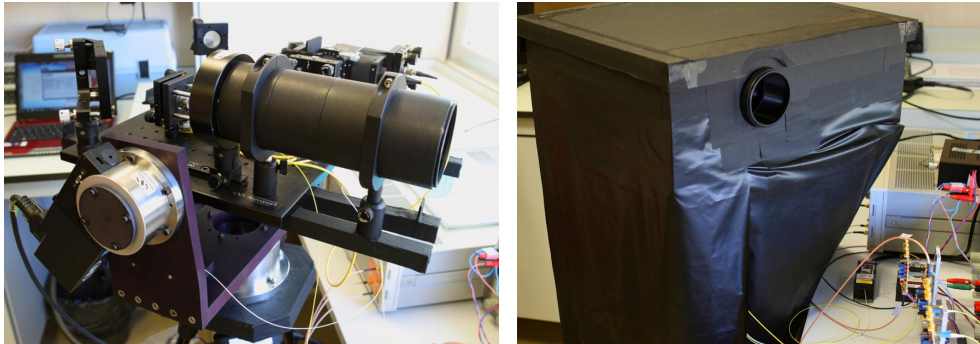
The reduction in background was characterised for just the tube placed in Alice first, and for both the tube and the blackout material later. Although considerable deviations were found in the measurements (due to the random changes in solar background and the difficulty characterising the background rate with and without the tube and box under exactly the same background conditions), the reduction in background was clear, especially in the second case when both tube and shield were put in Alice, when an average reduction of 6 dB was found.



**Figure 3.24** – AutoCAD design (left) and picture (right) of the gimbal system for the transmitter. Two high precision DC motors —a lateral and a base motor represented in the figure by LM and BM— provide the azimuth and elevation movements required for the alignment between Alice and Bob.



**Figure 3.25** – Alice mounted on a robust tripod.



**Figure 3.26** – Pictures of the transmitter with the antireflective tube (left) and with the shielding fabric and card (right).

### 3.9 Conclusions

In this chapter the electronics and optical setup of the transmitter module have been discussed.

To achieve high transmission rates Alice uses a fast GHz pulse pattern generator that generates the initial sequence of electrical pulses used to drive the two VCSELs. Each laser output is then attenuated so that a mean photon number of much less than one photon per pulse is achieved. This ensures that

with high probability only one photon encoding the same bit will be sent to the receiver, which is crucial for the security of QKD systems.

The laser sources were two GaAs VCSELs designed for an emission wavelength of  $\lambda \sim 850$  nm and a maximum bit rate of 4.25 Gbps. They were soldered on two driving boards containing a bias generator, a laser modulator and an automatic power control. An optimisation of the driving conditions of the VCSELs regarding their contribution to the quantum bit error rate was performed. The optimal bias current obtained was 2 mA and the optimal modulation current  $\sim 6$  mA, with a contribution to the QBER less than 0.5% at a clock frequency of 1 GHz. Besides, the spectral behaviour of both lasers was studied, resulting in a wavelength shift of  $\sim 0.15$  nm/mA of bias current. However such shifting was not a matter of concern since the system would be operating at a fixed bias level. Overall, the spectrum hardly changed with modulation current, clock frequency or time.

The polarisation extinction ratio of the light transmitting through each  $\lambda \sim 850$  nm channel was measured for different angles of incidence at different points throughout the transmitter. It was found out that certain optical components degraded the linearity of the polarisation states, affecting above all the diagonal state. A quarter-wave plate was used to counteract such effect. After that, extinction ratios of  $\sim 7000 : 1$  and  $\sim 4000 : 1$  for the vertical and diagonal polarisation states respectively were achieved.

To synchronise emitter and receiver Alice sends out a periodic bright pulse at a wavelength of 1550 nm and at a repetition rate of 10 MHz. The synchronisation signal at the emitter was obtained from the trigger output of the pulse pattern generator, which served as driving signal for the  $\lambda \sim 1550$  nm synchronisation VCSEL.

An important issue for an efficient reception of the key is the alignment of the three beams in Alice module. The coincidence of the three beams in the far field was performed by using a curved mirror and a CCD camera placed at its focal length.

Finally, the transmitter's optics was mounted on a high-precision gimbal system for its alignment with the receiver unit, and the whole structure was covered with blackout material to reduce the amount of stray light that may be collected by Alice.



# Chapter 4

## Free space as the quantum channel

The transmission channel is the physical medium that transports the quantum states encrypting the binary data between the sender and receiver of the QKD system. It has the fundamental role of preserving the quality of such quantum states, hence the name it sometimes receives as the *quantum* channel. Sending photons over a free-space link faces several challenges that need to be considered, such as the influence of everyday atmospheric conditions (rain, fog, snow, etc.). The transmission efficiency of the atmosphere is usually referred to as *atmospheric extinction*, which includes the interaction with air molecules, aerosol particles and water droplets through scattering and absorption. Additionally, atmospheric turbulence leads to inhomogeneities in the refractive index of the air, which can cause beam spreading, beam wander and scintillation, which are often translated into variations in the signal intensity at the receiver. Also the effect of background radiation coupling into the receiver telescope results in an increased error rate. This chapter is intended to briefly review the relevant aspects concerning free-space communication. The optical components used in transmitter and receiver to optimise the propagation of the beams through the atmosphere and enhance the detection

efficiency are also described. The calculation of some important parameters such as the attenuation of the link or the beam size at the receiver's end, are also discussed in this chapter.

## 4.1 Factors affecting free-space QKD

The quantum channel of the QKD system presented in this thesis is free space, i.e., photons carrying information encoded in their polarisation state propagate through the air from the sender to the receiver. To minimise the error rate of the key transmission it is fundamental that the transmission medium preserves such quantum states. Fortunately, the atmosphere is essentially a non-birefringent medium, thus enabling QKD protocols based on polarisation coding. Another advantage is the very low absorption coefficient of the atmosphere in the near-infrared window between  $\lambda \sim 830$  nm and  $\lambda \sim 860$  nm, ensuring high transmission efficiencies. There is however a limiting factor, which is the need of a free line of sight between emitter and receiver. The dependence of the transmission efficiency on weather conditions constitutes also a major challenge in free-space communication systems. In the following, the main factors affecting the performance of free-space quantum key distribution are discussed.

### 4.1.1 Line of sight requirement between Alice and Bob

As mentioned above, free-space QKD requires line of sight (LOS), which simply means that sender and receiver at their respective locations can see each other. As optical beams propagate and diverge in a linear way, the LOS requirement is less strict when compared to microwave systems, which need more area free from obstacles to take into account the extension of Fresnel zones.

In order to determine whether line of sight exists between two remote locations, visual observation is the easiest approach. For long distances ( $>1$  km), visual observation is not so trivial, and it can be necessary the use of field glasses and telescopic lenses. Also a variety of GIS (Geographic Information Systems) mapping software can be found to allow determining whether line

of sight exists between two known locations. Such programs can load high-resolution 3D topology maps, which include information regarding buildings and their specific locations.

Rooftop to rooftop is a typical deployment scenario in conventional communications. Additionally, when the roof access is not available or convenient, it might be possible to locate the transmitter and receiver modules indoor behind windows. If the former option is chosen, the delicate equipment of QKD systems should be carefully isolated from external harshness. In the case of the QKD system discussed in this thesis, the second scenario was chosen, and Alice and Bob were placed behind windows in their respective locations. However, special attention has to be paid to the angle the beam makes with the window: the more perpendicular the incidence, the lower the bounce-back of the beam. Moreover, it should be taken into account that some windows contain glass coatings to reduce glare, and are often specifically intended to reject infrared. Such coatings could reduce the signal by 60% or even more.

In spring and summer measurement campaigns, experiments were carried out with the windows open. However, in winter campaign Alice's window had to be closed to reduce the effect of turbulence on the beam caused by the difference of temperatures between the inside and outside, as discussed in the following subsection. That measure did not constitute a major problem since the additional loss introduced by the window was considered for the attenuation that had to be applied to the lasers in order to achieve the single-photon regime.

#### 4.1.2 Sources of loss

In QKD each emitted photon carries one bit of information, and thus, one obvious way of achieving high transmission rates is through minimising the losses of the quantum channel and the receiver. Therefore a careful characterisation of each contribution to the total loss was performed. The protocol used in these experiments, the B92, is especially sensitive to loss, as it was discussed in section 2.2.3, and hence the importance of properly characterising the losses.

One source of loss in a free-space optical system is due to the imperfection of the optical components, that is, *optical loss*. The amount of this loss depends on the characteristics and quality of the equipment. This value has been characterised in Alice, and it is taken into account for the total attenuation applied to the lasers output to reach an average photon number per pulse  $\mu$  of 0.1. The loss of the receiver optics was characterised to be  $\sim 8.6$  dB, including the coupling of the signal into the optical fibres (see section 5.6). Several other causes of loss that can occur in a typical free-space optical system are geometrical loss, pointing loss, and atmospheric loss.

*Geometrical loss* refers to the loss originated from the divergence of the optical beam. This loss is equal to the ratio of the area of the receiver collecting optics to the total area of the beam at the receiver. Alice's telescope has been designed to avoid geometrical loss for links lower than 3 km, as discussed in subsection 4.2.1, and therefore the contribution of this loss should be zero for links under this distance.

Moreover, if the transmitter does not accurately point to the receiver, an additional loss must be expected, the so-called *pointing loss*. The misalignment between both stations might happen due to building sway and thermal fluctuations. The influence of relative pointing deviations on the bit error rate and the key transmission rates achieved with the system presented in this thesis has been characterised in sections 6.3.4 and 6.3.5. The results show that the system is quite robust with a potential alignment maintained for 4 or 5 days without external intervention at a distance of 300 m. Nevertheless, since emitter and receiver are mounted on precise gimbal platforms for their alignment, a tracking process with high-precision motors will be implemented in the most coming future so that such effects can be compensated for. Examples of tracking systems that operate in free-space QKD implementations are described in [Schmitt-Manderbach, 2007] and [Gorman, 2010].

In a free-space optical link different atmospheric phenomena such as absorption, scattering and turbulence, may perturb and attenuate the signals that propagate through it. It must also be stressed that all these effects are weather dependent. They are described in more detail in the following subsection.



### 4.1.3 Atmospheric effects on beam propagation

The atmosphere is composed of oxygen and nitrogen molecules, and depending on weather, of large amounts of water vapour as well. Pollution adds other constituents to the atmosphere, especially in big cities and industrialised regions. Infrared photons propagating through the air can be scattered or absorbed by these particles. However, by selecting the right transmission wavelength, it is possible to benefit from optimal atmospheric windows. The QKD system discussed in this thesis operates at a wavelength of 850 nm, where fortunately the existence of a low absorption window coincides with the availability of commercial, high-efficiency single-photon detection modules, as already mentioned in section 3.3.2.

Overall there are three main atmospheric factors affecting optical wave propagation: scattering, absorption and turbulence (refractive index fluctuations). The attenuation of beams due to absorption and scattering is described by Beer's Law [Houghton, 1986, Ch.2], while turbulence is described by Navier-Stokes equations [Mikulevicius et al., 2004], [McDonough, 2004], or also by the simplified Kolmogorov's statistical approach [Kolmogorov, 1941]. In general, absorption and scattering cause attenuation of electromagnetic radiation, which depends on the wavelength. The transmission,  $\tau$ , of radiation through the atmosphere as a function of distance,  $z$ , is given by Beer's Law as

$$\tau = \frac{I(\lambda, z)}{I_0(\lambda)} = \exp(-z\gamma(\lambda)) , \quad (4.1)$$

where  $I(\lambda, z)$  is the intensity of the radiation at the distance  $z$ ,  $I_0$  is the intensity at the origin, and  $\gamma$  is the attenuation coefficient, which is a sum of four individual weather-dependent parameters —molecular and aerosol scattering coefficients,  $\alpha_m$  and  $\alpha_a$ , and molecular and aerosol absorption coefficients,  $\beta_m$  and  $\beta_a$ — and is given by

$$\gamma = \alpha_m + \alpha_a + \beta_m + \beta_a , \quad (4.2)$$

that is, the total attenuation is caused by the combined effect of different scattering and absorption phenomena, which are further divided according to

the size of interacting particles: molecular (smaller) or aerosols (larger particles).

## Scattering

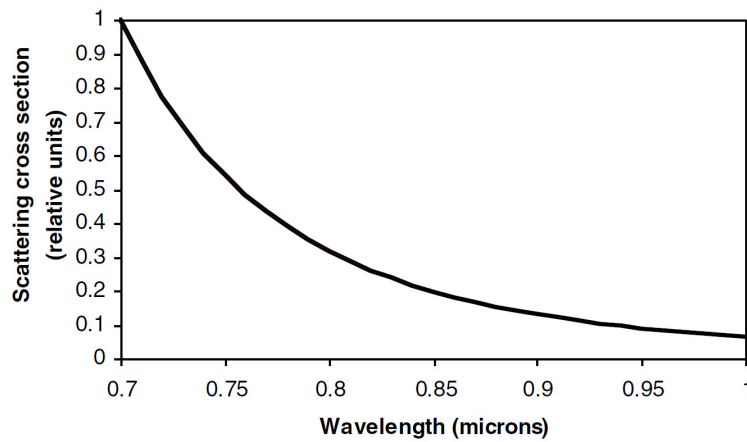
Scattering can be understood as a redirection of photons when they interact with other particles in the atmosphere, which can lead to a significant reduction of the signal intensity at the receiver's location. There are several scattering regimes depending on the size of the atmospheric particles that interact with the light. For particle radius  $r \ll \lambda/2\pi$ , the scattering is in the Rayleigh regime; for  $r \approx \lambda/2\pi$  the scattering is in the Mie regime; and for  $r \gg \lambda/2\pi$  geometrical optics can be used to study the scattering process. According to this description, fog is the main cause of beam attenuation due to scattering, since the average radius of fog particles is similar in size to the infrared wavelengths typically used in free-space optics. Rain and snow particles are larger than fog particles, thus being much less of an obstacle to the beam.

*Rayleigh scattering* takes place when a charge imbalance is induced by the optical radiation incident on the bound electrons surrounding a gaseous molecule. The electrons oscillate at the frequency of the incident beam and reradiate the light as a scattered wave. Particles involved in Rayleigh scattering are air molecules and haze. The scattering coefficient is proportional to  $\lambda^{-4}$ , what means that long wavelengths are less scattered than short wavelengths. Figure 4.1 represents this wavelength dependence of the Rayleigh scattering cross section in the infrared spectral range.

The implemented QKD system transmits the key at a wavelength of 850 nm and the synchronisation signal at a wavelength of 1550 nm, both moderately affected by Rayleigh scattering.

*Mie scattering* occurs for particles comparable in size with the transmission wavelength, being fog, haze and aerosol particles the main contributors to this scattering process in the near-infrared wavelength range. To assess the amount of light extinction due to Mie scattering it is necessary to know the composition, concentration, and size distribution of the atmospheric particles. In the case of aerosols, factors like location, time, wind velocity, or relative humidity must be considered. As this implies significant experimental complexity,

empirical models have been formulated describing aerosol conditions as a function of wavelength and visibility, the latter depending on local environmental parameters. However, if the exact theoretical formula describing Mie scattering is simulated by precise numerical methods, the dependence obtained of the attenuation coefficient with the wavelength in the infrared spectral range is not very drastic. By empirical observation it can be concluded that the highest beam attenuation is mainly due to Mie scattering caused by fog, and that it is accentuated when the distance increases.

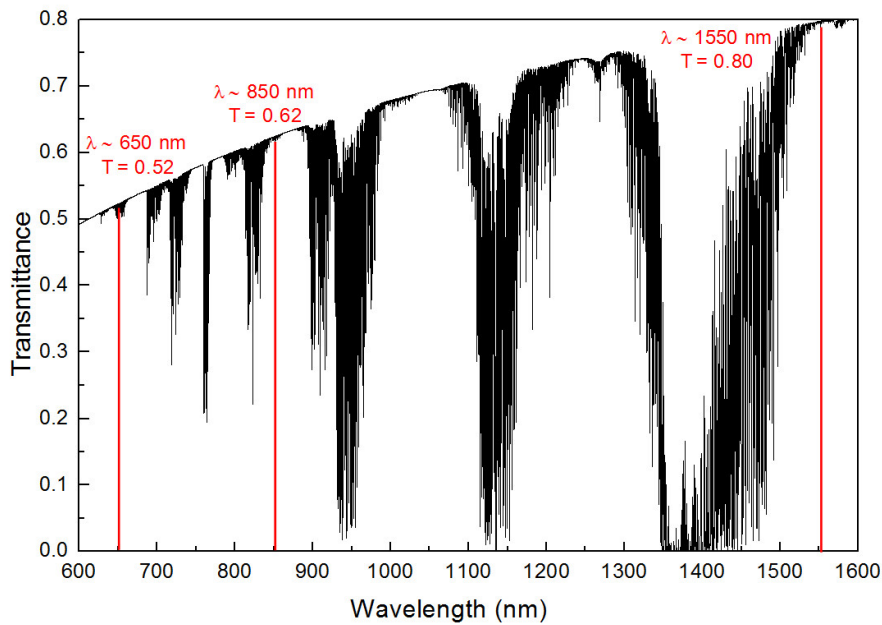


**Figure 4.1** – Rayleigh scattering cross section as a function of wavelength (after [Willebrand et al., 2002, Ch.3]).

## Absorption

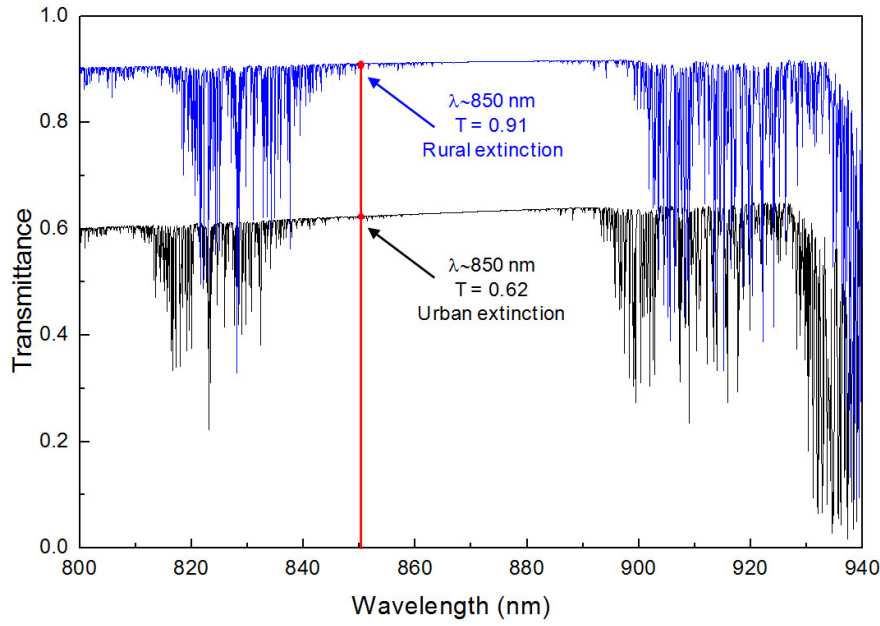
When photons interact with atmospheric molecules, these absorb part of the energy from the incident photons. This quantum process is known as absorption, which alters the electronic, vibrational, and/or rotational state of the molecule, thus producing the typical absorption spectra of molecules with a series of discrete absorption lines. The shape of these lines depends on several line-broadening effects, such as Doppler broadening and pressure broadening [Wallace et al., 2006, §4.4.3]. In the infrared atmospheric window most of the absorption is caused by water, carbon dioxide and ozone, being water vapour the primary molecular absorber in the near infrared range. It is evident that the attenuation of a signal will strongly depend on the number of absorbing particles. Given a specific wavelength, its corresponding extinction coefficient

can be computed by taking into account the type of particles present in the atmosphere and the information obtained from experimental molecular spectra. The transmission spectrum under a standard urban atmosphere—in our case aerosol concentration with 5 km visibility—was obtained by using the simulating atmospheric transmission computer code MODTRAN [Anderson et al., 2000]. As it can be seen in Figure 4.2, the simulation using this code resulted in transmittances of 0.52, 0.62 and 0.80 for the wavelengths of 650 nm (red was used for alignment purposes), 850 nm (key distribution) and 1550 nm (synchronisation signal), respectively. The transmission spectrum can also be computed with other atmospheric transmission programs, such as LOWTRAN or FASCODE [Anderson et al., 1995]. Both MODTRAN and LOWTRAN are band models and provide spectra of lower resolution than FASCODE, which is a line-by-line model.



**Figure 4.2** – Atmospheric transmittance as a function of wavelength under urban aerosol conditions and a visibility of 5 km (data simulated with MODTRAN 4.0).

Figure 4.3 shows the transmission spectra under both, urban aerosol conditions and rural conditions, where different extinction of the signal at the wavelength of 850 nm for both scenarios can be observed.



**Figure 4.3** – Atmospheric transmittance versus wavelength considering two types of aerosol scenarios: rural extinction with a visibility of 23 km and urban extinction with a visibility of 5 km (data simulated using MODTRAN 4.0).

## Turbulence

Turbulence in the atmosphere has a considerable effect on the transmission of a beam over a free-space link. Small variations in temperature ( $< 1^\circ\text{C}$ ) lead to changes in the wind velocity (*eddies*). The derived changes in the atmospheric density give rise to a variation of the index of refraction on the order of  $10^{-6}$ . As a result, the light modifies its path while propagating through the air. Since these inhomogeneities in the refractive index are variable in time or in space, the changes in the index of refraction seem as turbulent behaviour to the outside viewer.

Depending on the ratio between the size of the atmosphere's eddies and the beam size, three different phenomena may appear under turbulence. The beam can be deflected, leading to *beam wander*, when turbulent eddies are large compared to the beam diameter. When turbulent eddies are small compared to the diameter of the beam they give rise to scattering, producing *beam spreading* in a higher order than diffraction theory predicts. The use of large optics and

a large beam diameter can compensate partly for these effects. On the other hand, fluctuations in the received intensity, caused by small variations in the optical path, which can produce destructive or constructive interference, are known as *scintillation*. Although turbulence is not a time-invariant, easy-to-model phenomenon, various approaches have been proposed. The most used and verified is the Kolmogorov model [[Friedlander et al., 1961](#)].

During the measurement campaigns for the characterisation of the QKD system presented in this thesis, the three effects above mentioned could be observed. Of the three turbulence effects, scintillation might possibly be the most frequent. A possible solution to mitigate this effect in astronomical telescopes and, recently, in free-space optical systems has been the use of adaptive optics, such as deformable mirrors. Similarly, QKD implementations that employ adaptive optics have also been reported [[Capraro, 2008](#)], [[Capraro et al., 2008](#)], [[Chapuran et al., 2009](#)], [[Safari et al., 2009](#)], although there are still some limitations to the use of these systems.

Regarding beam spreading, a diameter almost double than that calculated was measured at a distance of  $\sim 300$  m from the sender. However, it cannot be asseverated that lack of precision in the collimation technique was not in part the cause of such effect. In summer measurement campaign, a displacement of the beam centre of more than 2 cm for a 300-m link could be observed when turning the air conditioning on in the transmitter location. Since emitter and receiver were located inside their respective buildings, the temperature difference between the inside ( $\sim 20^\circ\text{C}$ ) and outside ( $>30^\circ\text{C}$ ) created great turbulence at the window frontier. When the air conditioning was off, this beam wander could barely be perceived. The opposite situation occurred in winter: low temperatures outside ( $<10^\circ\text{C}$ ) and  $\sim 20^\circ\text{C}$  inside caused even a more perceivable beam wander effect than in summer, which was especially noticeable after sunset. In this case the turbulence due to the difference of temperatures was solved by closing the window in Alice's location, thus avoiding the air flow which caused the turbulence at the origin of the beam. This measure did not cause additional losses since, as already mentioned, the loss introduced by the window was taken into account for the attenuation applied to the VCSELs. Another way of overcoming beam wander is by slightly defocusing the beam to increase the beam diameter so that it always overlaps the receiver's aperture.

However, this of course causes additional losses in the system. Since the beam wander takes place over relatively long time scales, it can be compensated by actively tracking the transmitter and receiver.

#### 4.1.4 Weather conditions

One disadvantage of free-space setups resides in the dependence of the transmission on weather conditions. While with clear air the attenuation at  $\lambda \sim 850$  nm can be lower than 0.2 dB/km, it rises to 2–10 dB/km in case of moderate rain, up to 20 dB/km under heavy rain, and up to 100 dB/km in clouds [Kim et al., 2001b], [Grabner et al., 2011]. However, the impact of rain is significantly much lower than that of fog, which can cause the attenuation to increase over 300 dB/km [Kim et al., 2001a]. The reason is that raindrops (with radii between 200 and 2000  $\mu\text{m}$ ) are considerably larger than the wavelength of commonly used free-space laser sources.

In snow weather conditions absorption of infrared wavelengths also takes place, although scattering is not a major problem since the size of snowflakes is large when compared to infrared wavelengths. The shape and size of ice crystals constituting snowflakes vary, but usually they are larger than rain particles. Typically, the attenuation caused by light snow in beam propagation varies from 3 dB/km to 30 dB/km, which is more than light rain and less than moderate fog.

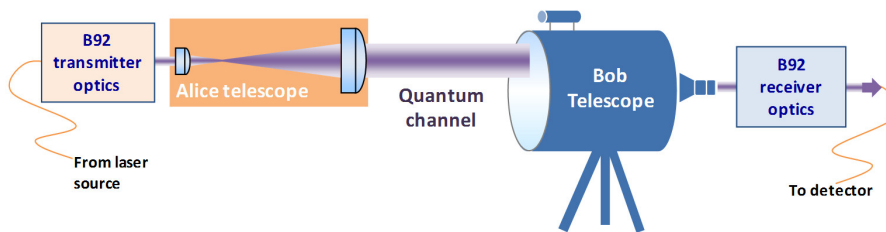
Fog is the worst-case scenario in terms of laser transmission since it is composed of small water droplets with radii similar to the wavelengths in the near infrared. The particle size distribution depends on the degree of fog. When visibility lies between 0 and 2 km, weather conditions are considered as fog. If instead of visibility a more quantitative definition of foggy conditions is required, particle size or density measurements are employed. Physical characterisation of fog is a very complicated task, and the theory of fog process is not well understood yet. Factors like the height may modify the density distribution of fog particles, making more complex the theoretical modelling of fog. Indeed, the limited amount of information regarding the local impact of fog on the availability of free-space optical systems is certainly one of the prime challenges for the field.

### 4.1.5 Background light

Background light couples into the receiver telescope leading to more background noise and an increased error rate. The errors generated by the background light can be reduced to a reasonable level by using a combination of spectral, spatial and temporal filtering. Some free-space QKD systems that implement efficient methods to reduce background radiation, enabling the operation in daylight conditions, have been demonstrated in [Benton et al., 2010], [Hughes et al., 2002b]. Spectral and spatial filtering are implemented in the QKD system discussed in this thesis by means of a 1-nm interference filter and  $62.5\text{ }\mu\text{m}$ -diameter optical fibres, respectively. This will be further discussed in chapter 5. Additionally, careful shielding of emitter and receiver units with blackout material greatly contributes to reduce the level of background radiation that couples into the system.

## 4.2 Free-space optics used in the QKD system

A schematic of the free-space optical link is shown in Figure 4.4. To enable Bob to collect as many photons from Alice as possible, two telescopes are installed, one at each end of the QKD system. In the following subsections, the telescopes of sender and receiver, and the optical equipment needed to enhance the total efficiency of the link, are described.



**Figure 4.4** – Schematic of the free-space optics used for the QKD link.



### 4.2.1 Design of the transmitter telescope and collimation of the output beam

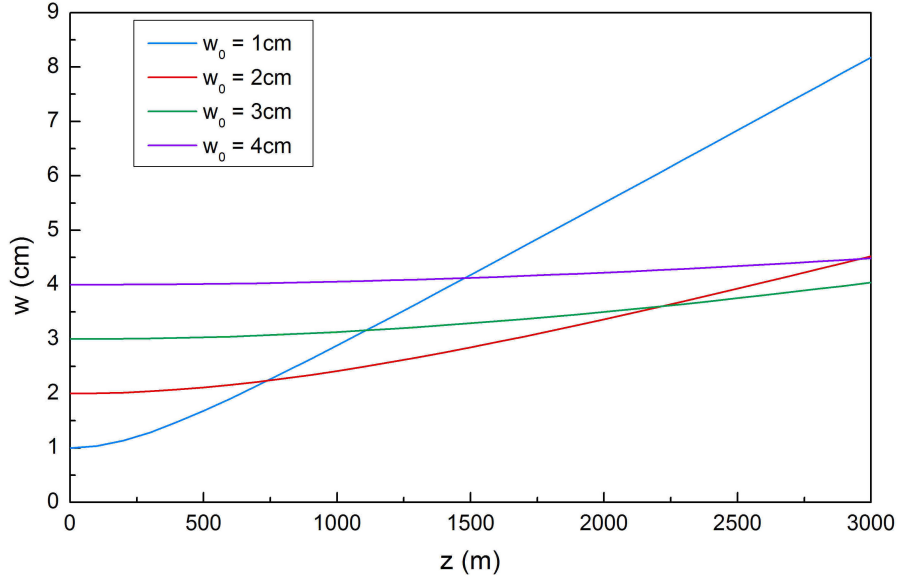
On Alice's side the telescope consists of two achromatic doublet lenses. The choice of the lenses was done according to several factors, such as the transmission distance of the link, the receiver telescope and the off-the-shelf availability. On the receiver's side a Schmidt-Cassegrain telescope is used to focus the beam from the transmitter. Due to the design of a classical Cassegrain telescope the secondary mirror limits the diameter of the received beam, in our case to less than 90 mm. Regarding the distance of the optical link, it was initially thought to be close to  $\sim 3$  km for key distribution in urban radii. The maximum achievable transmission distance of the system is discussed in more detail in section 6.5.

In order to reduce the effects of Gaussian beam divergence, the beam coming out of Alice had to be expanded and collimated. The radius  $w$  (to the  $1/e^2$  of the intensity) of a Gaussian beam as a function of distance  $z$  is defined as

$$w(z) = w_0 \sqrt{1 + \left(\frac{z}{z_R}\right)^2}, \quad (4.3)$$

$z_R$  being the Rayleigh length, and  $w_0$  the beam waist [Menzel, 2007, §2.4]. The Rayleigh length is in turn given by  $z_R \cong \pi w_0^2/\lambda$ . Figure 4.5 represents the radius of the beam  $w$ , as a function of the propagating distance  $z$  at a wavelength of  $\lambda \sim 850$  nm, for different initial beam radius at the emitter's aperture,  $w_0$ .

The chosen diameter of the output beam at Alice was  $\approx 40$  mm ( $w \approx 20$  mm), since at a distance of 3 km the beam was still sufficiently small to be coupled into the receiver telescope, and the availability and cost of the lenses to be used were within reasonable margins. Therefore two lenses were used to expand and collimate the  $\sim 7$  mm-diameter beams coming out from the fibre-coupled collimators (see Figure 3.1), to an approximately 40 mm-diameter gaussian beam, which is then transmitted through free space to the receiver telescope. The first lens focuses the beam to a diameter of  $13.82 \mu\text{m}$  while the second lens, placed at its focal length from the waist of the beam, expands the beam to a 39.15 mm-diameter collimated beam.

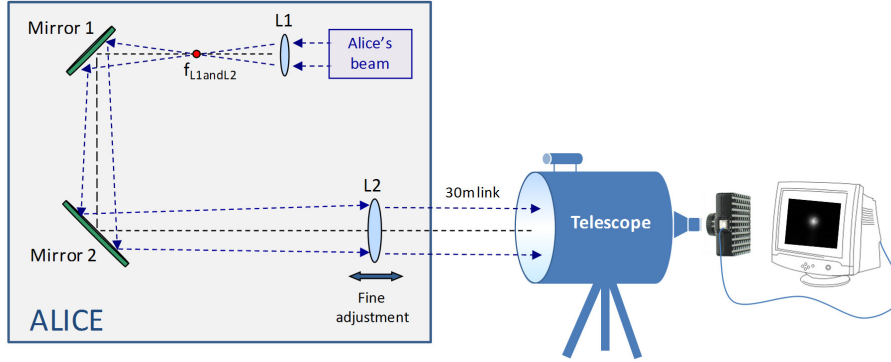


**Figure 4.5** – Beam radius  $w$  against the propagation distance  $z$  for several values of the beam waist at the transmitter aperture  $w_0$ .

The linear approximation for the divergence of the beam is given by the equation  $\theta \simeq \lambda/\pi w_0$  [Menzel, 2007, §2.4]. Using this equation with a 39.15 mm-diameter Gaussian beam yields a total angular spread of the beam of  $2\theta = 13.82 \mu\text{rad}$ , which corresponds to the beam diameter being broadened by 52.56 mm over the 3 km link —resulting in a beam diameter of 91.71 mm—. For comparison purposes, if no telescope had been used in the sender, the  $\sim 7$  mm beam out of the collimators with a divergence of  $\theta = 77.75 \mu\text{rad}$  would have produced a beam diameter of  $\sim 466.5$  mm at the receiver at 3 km.

In order to ensure that the output beam was collimated, i.e., that the second lens was placed at its focal length from the focal plane of the first lens, a collimating technique using the Schmidt-Cassegrain telescope was carried out. It consisted in firstly placing a CCD camera at the focal length of the Schmidt-Cassegrain telescope. This was achieved by imaging the moon at the focal plane. The exact focus of the telescope was thus found. Then the beam from Alice was directed to Bob's telescope at a distance of 30 m. Parallel rays cross at the focal point when passing through a lens or any other converging optics and therefore, if the beam from Alice was well collimated, the size of the focus at Bob's telescope would be minimum. Therefore, this spot was minimised on the CCD camera by changing the position of Alice's second lens,

L2, in relation to the first lens, L1. A schematic of this collimation technique is illustrated in Figure 4.6.



**Figure 4.6** – Collimation method of Alice's output beam using the receiver telescope and a CCD camera. The position of the lens L2 is adjusted until the smallest spot on the CCD camera is achieved.

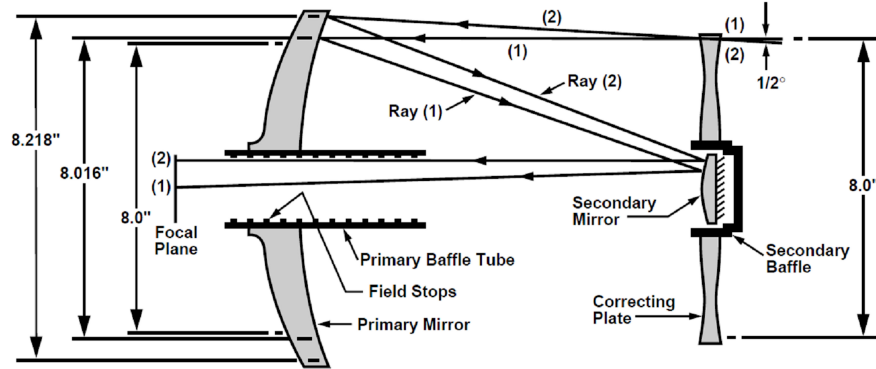
However, perfect collimation of the beam at short distances was not necessary provided that the diameter at the receiver telescope was smaller than 90 mm (to ensure the secondary mirror of the Schmidt-Cassegrain telescope did not block the incoming beam).

Although the two lenses of the transmitter telescope were achromatic, there was still some aberration due to the spectral separation between  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm. Therefore, as the collimation process was performed for the  $\lambda \sim 850$  nm signal, the  $\lambda \sim 1550$  nm beam diverged due to chromatic aberration since only one optical path existed for both wavelengths. This fact resulted in extra loss for the synchronisation signal, as it reached the receiver larger than expected. As already discussed in section 3.5, such loss did not represent a major problem, given that the power at the receiver exceeded the sensitivity of the timestamp card.

#### 4.2.2 Receiver telescope

On the receiver's end the beam from Alice is collected by a Schmidt-Cassegrain telescope. It is a Meade LX200ACF model with a diameter of 25.4 cm, an equivalent focal distance of 2.5 m and fine-pointing capability. It also includes a GPS to facilitate a quick and precise alignment of the telescope. A Schmidt-

Cassegrain telescope is composed of a primary and a secondary mirror. The former is a spherical mirror and its spherical aberration is rectified by a thin lens with 2-sided aspheric correction. The latter is a convex mirror. A diagram of the Meade 8" LX200GPS model is depicted in Figure 4.7, similar to the 10" model used in the proposed QKD system.



**Figure 4.7** – Diagram of Meade Schmidt-Cassegrain 8 inch LX200GPS (after [Meade, 2003]). Not to scale.

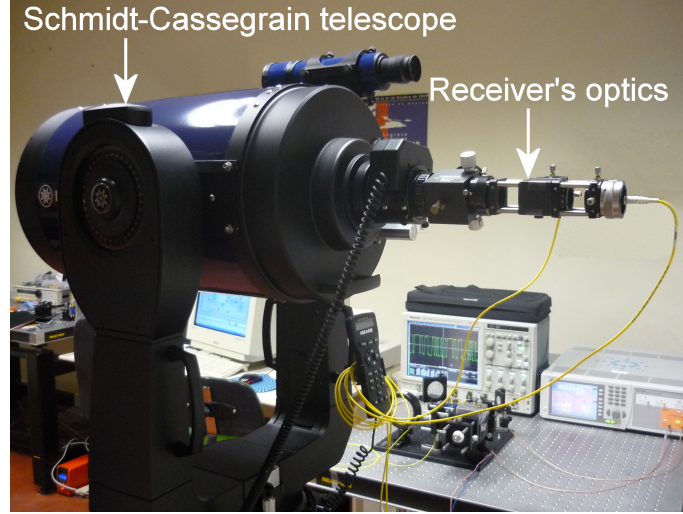
In the Meade Schmidt-Cassegrain optical system shown [Meade, 2003], light enters from the right, passes through the correcting plate, proceeds to the primary mirror, and then to the secondary mirror. The convex secondary mirror multiplies the effective focal length of the primary mirror and results in a focus at the focal plane, with light passing through a central perforation in the primary mirror.

Bob's optics has been designed to be directly coupled to the output of the telescope by using lightweight and compact mounts, as shown in Figure 4.8. In the following subsection it will be discussed how the  $\lambda \sim 850$  nm beam propagates from Alice's optics to Bob's telescope, and how it is efficiently coupled into the receiver's optical fibres.

### 4.2.3 Optical path: from the laser sources to the detectors

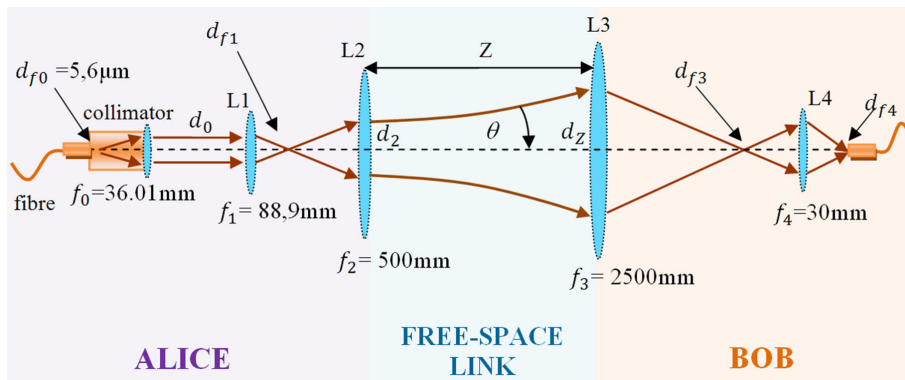
A schematic of the free-space optics of the whole QKD system is shown in Figure 4.9. The aim of the diagram is to show the optical path of the Gaussian beam from the transmitter's side through the free-space link to the receiver. A

5.6  $\mu\text{m}$  single-mode optical fibre is used in Alice to spatially filter and couple the laser output into a collimator to provide a collimated free-space beam (only one fibre and one collimator are represented in the schematic for simplicity purposes).



**Figure 4.8** – The Schmidt-Cassegrain telescope with Bob's optics attached to it.

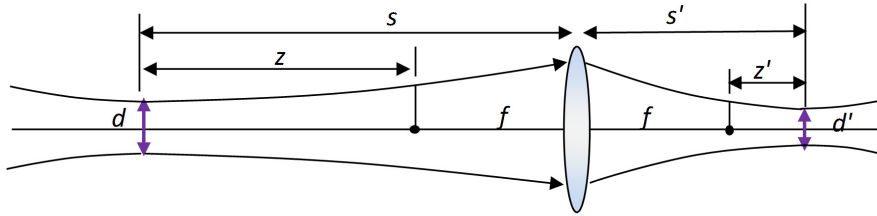
The beam is then expanded with L1 and L2, which are two doublet lenses that constitute the transmitter telescope described in section 4.2.1.



**Figure 4.9** – Setup of the free-space optics. L1, L2 and L4 are three achromatic doublet lenses; L3 is the Schmidt-Cassegrain telescope;  $f_0$ ,  $f_1$ ,  $f_2$ ,  $f_3$  and  $f_4$  are focal lengths;  $d_{f0}$ ,  $d_{f1}$ ,  $d_{f3}$ ,  $d_{f4}$ ,  $d_0$ ,  $d_2$  and  $d_z$  are beam diameters;  $Z$  is the length of the link; and  $\theta$  is the beam divergence angle.

On the receiver's side, L3 is a lens that represents Bob's telescope with the same equivalent focal distance, and L4 is a 30 mm focal length doublet lens used to improve the coupling of the beam into the optical fibre that conveys the photons to the photodetectors.

When a Gaussian beam passes through an optical system, its waist is modified. Diffraction instead of paraxial equations determines the size and location of the new waist. In [Siegman, 1971] matrix transformations are used to study Gaussian beam propagation through lenses and mirrors. A quite useful approach to this problem has been developed in [Self, 1983], where a method to model the transformations suffered by a laser beam through simple optics is presented. It consists in calculating the Rayleigh range and the beam waist location following each individual optical element. For comparison with the geometrical optics case in calculating the focusing effect of a thin lens, the waist of the input beam is regarded as the object, and the waist of the output beam as the image. The situation for a positive lens with real object and image beam waists is shown in Figure 4.10.



**Figure 4.10** – Geometry of the imaging of a Gaussian beam by a lens, shown for the case of a positive lens and real object and image waists.

The new beam parameters are then calculated using a formula analogous to the well known standard lens formula, which includes the Rayleigh range of the incident beam [Smith, 2000]:

$$\frac{1}{s + z_R^2/(s - f)} + \frac{1}{s'} = \frac{1}{f}, \quad (4.4)$$

where  $s$  and  $s'$  are the distances from the waist of the input and output beams to the lens, respectively,  $f$  is the focal length of the lens, and  $z_R$  is the Rayleigh range of the original beam. The waist and focus are not at the same locations, and if the beam is weakly convergent they can be quite separated. The

calculation of the size and location of the new waist can be made, respectively, by means of the following equations:

$$w_1^2 = \frac{f^2 w_0^2}{z^2 + \left(\frac{\pi w_0^2}{\lambda}\right)^2}, \quad (4.5)$$

$$z' = \frac{-zf^2}{z^2 + \left(\frac{\pi w_0^2}{\lambda}\right)^2}, \quad (4.6)$$

$w_0$  being the radius (to the  $1/e^2$  points) of the original waist,  $w_1$  the radius of the new waist,  $z$  the distance from the first lens focal point to the plane of  $w_0$ , and  $z'$  the distance from the second lens focal point to the plane of  $w_1$ . In the special case where  $s = f$ , the equation providing the new waist size reduces to:

$$w_1 = \frac{\lambda f}{\pi w_0}. \quad (4.7)$$

Using the above equations, the beam waists and their locations along the optical path depicted in Figure 4.9 have been calculated. The collimated beam diameter at the collimator output in Alice,  $d_0$ , can be calculated using Eq. 4.7 since the output of the fibre is located at the focal length of the collimator:

$$d_0 = \frac{4 f_0 \lambda}{\pi d_{f0}} = 6.96 \text{ mm}.$$

Note that  $d_0 = 2w_0$ . As the distance between the collimator and L1 is  $\sim 12$  cm, the beam diameter will be maintained along this path. Thus, again Eq. 4.7 can be applied to calculate the waist size of the beam after L1:

$$d_{f1} = \frac{4 f_1 \lambda}{\pi d_0} = 13.82 \text{ } \mu\text{m}.$$

As already mentioned, L2 placed at its focal length from the waist of the incoming beam (in this case it coincides with the focal plane of L1), will expand and collimate the beam into the following diameter:

$$d_2 = \frac{4 f_2 \lambda}{\pi d_{f1}} = 39.15 \text{ mm}.$$

The spot size at the receiver's end will be increased due to diffraction in the transmitter's aperture (L2). The QKD system under discussion was characterised for a 300 m link. Using Eq. 4.3, the diffraction limited spot after 300 m has a diameter of  $d_Z = 40.02$  mm. The new beam waist  $d_{f3}$  after the Schmidt-Cassegrain telescope and its distance  $z'$  to the focal plane of the telescope (see Figure 4.10) can be calculated for a link of  $Z = 300$  m using a variation of Eq. 4.5 and 4.6 respectively:

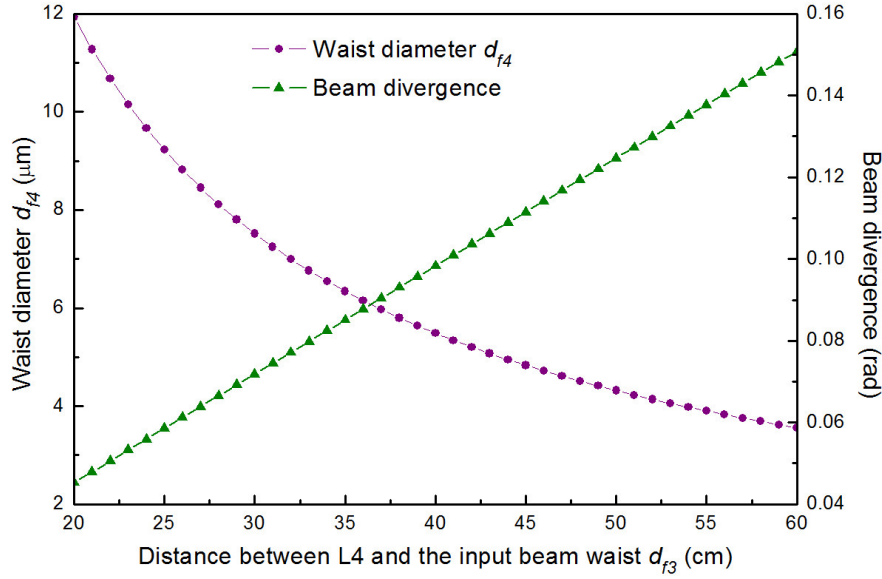
$$d_{f3} = d_2 \frac{f_3}{\sqrt{(Z - f_3)^2 + z_R^2}} = 67.63 \mu\text{m} ,$$

$$z' = \frac{(Z - f_3) f_3^2}{(Z - f_3)^2 + \left(\frac{\pi d_2^2}{4\lambda}\right)^2} = 0.89 \text{ mm} .$$

The beam then passes through Bob module (described in detail in chapter 5) and is coupled into two optical fibres (one for each polarisation state), which are then connected to the single-photon detectors. The optical fibres used in the setup have a core diameter of  $62.5 \mu\text{m}$ , which is a good compromise between easy coupling and spatial filtering of the background radiation. As the beam waist after the receiver telescope  $d_{f3}$  is larger than the core of the fibre, an additional lens L4 is employed to improve the coupling of the beam into the fibre (see Figure 4.9). The new size of the beam waist  $d_{f4}$  and its location depend on the distance between L4 and the location of the waist  $d_{f3}$  (which is almost coincident with the focus of the Schmidt-Cassegrain telescope). Such distance has to provide two conditions: a beam waist  $d_{f4}$  smaller than the core of the fibre, and a beam divergence well-suited to the fibre's numerical aperture. The  $62.5 \mu\text{m}$  optical fibre has a numerical aperture  $NA = 0.275 \pm 0.15$ . Therefore, considering the most restrictive value, the maximum beam divergence allowed is  $\theta = \arcsin(0.275 - 0.15) = 0.125$  rad. In order to establish the best location for L4, the diameter of the beam waist after L4 ( $d_{f4}$ ) and the beam divergence, were calculated as a function of the distance between L4 and the waist  $d_{f3}$  of the input beam. From Figure 4.11 it can be seen, that the maximum beam divergence allowed for the beam after L4 (0.125 rad as just above calculated) corresponds to a distance of  $\sim 50$  cm between L4 and  $d_{f3}$ . However, shorter distances have associated lower beam divergences and larger focus depths, making easier to place the fibre at the beam waist, and as a



result allowing a better coupling of the beam into the fibre. Shorter distances were achieved either by moving the focal plane of the Schmidt-Cassegrain telescope with the focus knob, or by displacing L4. The calculated waist diameters  $d_{f4}$  show that the beam waist requirement being smaller than the core of the optical fibre was widely satisfied.



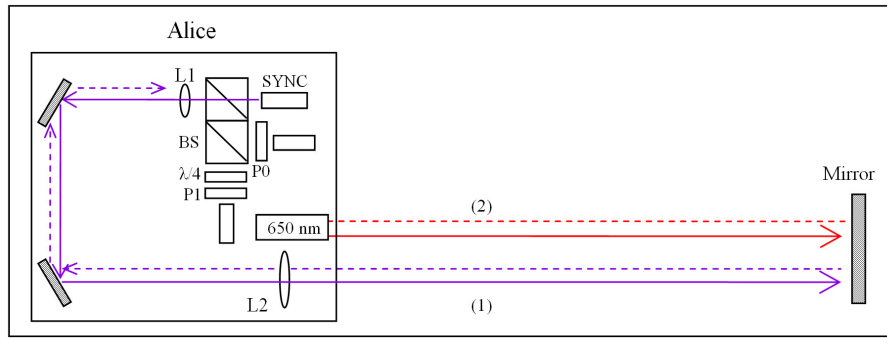
**Figure 4.11** – Waist diameter of the beam after lens L4 (left) and its divergence (right) against the distance between L4 and  $d_{f3}$ .

#### 4.2.4 Alignment of the transmitter and receiver telescopes

The technique implemented to align the telescopes of Alice and Bob consisted in propagating a visible laser beam at a wavelength of  $\lambda \sim 650$  nm through the same path as the  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm beams or parallel to it.

For short links the  $\lambda \sim 650$  nm laser was launched through the synchronisation channel as the red beam did not diverge much and could be perfectly observed at the receiver. For long links (hundreds of meters), launching the red laser through any of the data or synchronisation channels was not viable since the beam reached the receiver's end very divergent due to chromatic aberration. Therefore, for experiments at long distances, a parallel beam to the data and synchronisation beams was used to align both stations. This was done by launching the red laser output into an optical collimator via a pigtailed optical

fibre. The collimator was held by means of a kinematic mount and placed parallel to the  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm beams at a certain distance from L2, as Figure 4.12 shows. By fine tweaking the kinematic mount, the alignment beam was made parallel with the data and synchronisation beams. For this purpose a planar mirror was utilised, as represented in Figure 4.12. First, the mirror was oriented to make the reflected beam of the synchronisation channel reach the focus of L1 (step 1 in the figure). This ensured the surface of the mirror was perpendicular to the beam wavefront. Then the kinematic mount was adjusted for the reflected  $\lambda \sim 650$  nm beam to hit the same point in the collimator where it emerged (step 2).



**Figure 4.12** – Schematic of the method used to establish parallelism between the alignment beam ( $\lambda \sim 650$  nm) and the beams carrying information at  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm.

At 300 m the parallel red beam could perfectly be distinguished on a white screen placed at the aperture of the receiver telescope with a diameter of  $\sim 3$  cm. As the position of the  $\lambda \sim 850$  nm spot relative to the position of the alignment beam was known, Alice and Bob's telescopes could be coarsely aligned with this method. The fine alignment was later performed by maximising the detected optical power after Bob module, as will be further discussed in section 6.1.

### 4.3 Conclusions

The quantum states encoding the binary data of the key are transmitted through free space from sender to receiver. The atmosphere constitutes an ideal transmission medium as it is non-birefringent and therefore no

compensation is required to preserve the polarisation states of the photons. Moreover, the existence of a low absorption window in the proximity to  $\lambda \sim 850$  nm, where efficient single-photon detectors are available, makes this medium attractive for a QKD system.

However, there are some issues concerning a free-space channel that need to be addressed. One is the beam divergence, which has been taken into account by correctly designing the aperture of Alice's telescope. Regarding atmospheric attenuation, under urban aerosol conditions the attenuation at  $\lambda \sim 850$  nm is  $\sim 2$  dB/km. Turbulence in the atmosphere, especially at low altitudes and in urban areas, can lead to fluctuations of the beam position at the receiver. Although this effect in most cases is not a fundamental limitation, it might cause additional detection losses. Another aspect of free-space QKD systems that needs special attention is the background from the sunlight or other sources of ambient light, which may be collected by the receiver causing an increased error rate. Several techniques such as spectral, spatial and timing filtering can be applied to maintain a low error level.

Two telescopes have been installed, one at each end of the QKD system, in order to enable Bob to collect as many photons from Alice as possible. In addition to the Schmidt-Cassegrain telescope, two imaging lenses with 30 mm focal length have been mounted in the receiver module to enhance the beam coupling into the fibres. Finally, to facilitate the pointing between both stations, an additional visible laser at  $\lambda \sim 650$  nm is sent in parallel with the  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm beams.



## Chapter 5

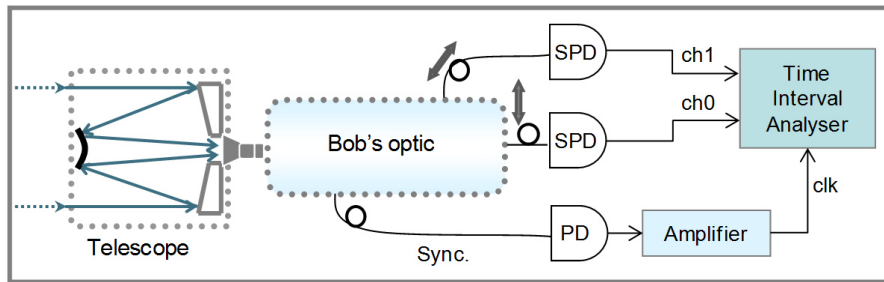
# Design and characterisation of the receiver

In this chapter the experimental setup of the QKD receiver is discussed. Firstly, a description of the optics is given, followed by the general features of single-photon avalanche diodes and a comparison to other detectors. Next, a description of the timestamp card used to record the arrival times of the photons coming from Alice is given. Moreover, the characterisation of the polarisation extinction ratio of the non-orthogonal quantum states at Bob is discussed as well as the measures taken to improve it. Then, the components involved in the detection of the synchronisation signal are described. Finally, the filtering and isolation methods to reduce the background radiation that couples into the receiver are presented.

## 5.1 Setup of the receiver

The receiver must have the capability of detecting single photons, analyse their polarisation and record their time of arrival. Figure 5.1 shows a schematic of the main parts of the receiver module. The beam of photons sent from Alice is collected by a Schmidt-Cassegrain telescope (described in section 4.2.2), which focuses it into a smaller beam waist. Bob's module contains the optics responsible for three key processes: the discrimination of the synchronisation signal at  $\lambda \sim 1550$  nm and the beam at  $\lambda \sim 850$  nm; the spectral filtering to remove the background radiation from the received signal; and the polarisation analysis of the incoming quantum states according to the B92 protocol. After the analysis of their polarisation, the photons are coupled into multimode optical fibres, and launched into two single-photon detectors (SPD). The output of each detector is connected to an input data channel ('ch0' and 'ch1') of the Time Interval Analyser (TIA), which time-tags the arrival of every detected photon. The synchronisation signal at  $\lambda \sim 1550$  nm is coupled into an optical fibre, and is detected and amplified by an InGaAs photodetector (PD) and a fast trans-impedance amplifier, respectively. The amplified signal is then connected to the external-clock input of the TIA.

The optics, the single-photon detectors and the timestamp card or TIA are further described in the following sections, as well as the ancillary processes such as synchronisation and filtering.



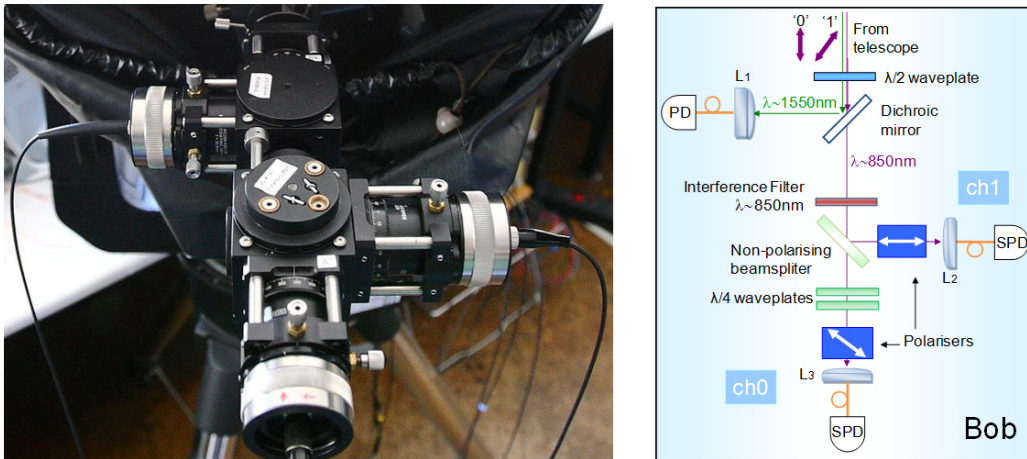
**Figure 5.1** – Diagram of the receiver. SPD are single-photon detectors, and PD is an InGaAs photodetector to detect the synchronisation signal.

## 5.2 Configuration of the optics module

As already mentioned, the B92 protocol is a two-state protocol, where the bits of the sequence sent by Alice are encoded into two non-orthogonal polarisation states. A suitable receiver will therefore require the ability to detect this type of signal encoding.

A photograph and a diagram of Bob's optics are shown in Figure 5.2. The receiver has been designed to be directly coupled to the output of the Schmidt-Cassegrain telescope via a standard 25 mm cage plate. The whole optomechanical module has been constructed as a cage assembly system, as shown in the picture of Figure 5.2.

The first component the photons encounter at the input of the receiver's optics is a half-wave plate, which is used to align the incident electric field of the vertical state with the optic axis of the dichroic mirror, so that the degradation of this polarisation state is minimised. The diagonal state is later recovered in 'channel 0' (ch0 in the figure) by means of two quarter-wave plates. The beam at  $\lambda \sim 850$  nm and the synchronisation beam at  $\lambda \sim 1550$  nm are spectrally discriminated by a dichroic mirror. The background radiation is filtered by using a narrow band-pass spectral filter centred at  $\lambda \sim 850$  nm. The spectral filtering will be further discussed in section 5.8.



**Figure 5.2** – Picture (left) and diagram (right) of the receiver's optics. SPD are single-photon detectors and PD is an InGaAs photodetector;  $L_1$ ,  $L_2$  and  $L_3$  are three doublet lenses used to couple the signals into the optical fibres.

The discrimination of the two non-orthogonal polarisation states encrypting the binary states ‘1’ and ‘0’ is achieved by using a non-polarising beamsplitter and two high-extinction polarisers. Provided the beamsplitter is of good quality and properly coated, the incoming photons are equally and randomly split between the two detector arms. In ‘channel 0’ (ch0 in Figure 5.2) the polariser is oriented orthogonally to the angle of polarisation of the state ‘1’, so that only the zeros are detected in this channel. On the other hand, in ‘channel 1’ (ch1 in Figure 5.2) the polariser is oriented against the state ‘0’, and thus only the ones can be detected in this arm. Such configuration provides with a deterministic measurement of the quantum states, albeit at the cost of losing 75% of the received photons: 50% of the incoming photons are lost since they will enter the incorrect channel and will be blocked by the polariser; and half of the remaining 50% that have entered the correct analyser arm will be blocked by the polarisers, since these form an angle of 45 degrees with the polarisation state to be detected in each channel. The advantage of this protocol compared to the BB84 is that only two quantum states are required and no basis reconciliation is needed.

With the help of two imaging lenses with a focal length of 30 mm, the photons are coupled into two 62.5  $\mu\text{m}$ -diameter multimode fibres (one for each polarisation), which are then connected to two Silicon *single-photon avalanche diodes* (SPADs), which emit an electrical pulse whenever a photon is detected. These ‘clicks’ created in the electronics of each SPAD are then recorded by a timestamp card, that is, the arrival times of the detected photons are logged. Both, the SPAD and the timestamp card, are described in the following.

### 5.3 Single-photon detection

One of the technological challenges of QKD is the detection of single photons. There exists a variety of devices capable of registering the energy of a single photon, which include photomultiplier tubes, superconducting transition edge sensors, superconducting nanowire sensors, avalanche photodiodes, parametric upconversion detectors, and single-photon detectors based on quantum dots and semiconductor defects. The most significant features that define the performance of single-photon detectors are listed in the following:



- *Detection efficiency*, which is mainly determined by the constituent materials of the detector.
- *Dark-count rate* or rate at which the detector registers events generated in the absence of an arriving photon.
- *Timing resolution*, given by the statistical distribution of delays from the time of detection of a photon and the generation of an electrical signal. Usually this is measured as the FWHM of the timing jitter of the signal.
- *Recovery time* or *dead time*, which is the interval of time that follows the absorption of a photon until the detector is able again to register a second photon. This time depends on the finite bandwidth of the device (due to various characteristics such as carrier transit times, parasitic capacitance effects, etc.), and the afterpulsing effect [Hiskett et al., 2001], [Cova et al., 1991].

An ideal detector from the QKD design point of view should have a low dark-count rate not to increase the quantum bit error rate, a short dead time allowing high data rates, a small timing jitter to ensure good timing resolution, and high detection efficiency, enabling the detection of as many photons as possible. Also, the ability to resolve photon number is a plus, because in the great majority of conventional single-photon detectors a multiphoton pulse triggers the same output signal as a single photon, what makes the QKD systems using these detectors vulnerable to a bright illumination attack (see subsection 2.4.3).

The *noise equivalent power* ( $NEP$ ) is a commonly used figure of merit for photodetectors, and it is defined as the optical power required to measure a unity signal-to-noise ratio. It takes into account the efficiency of the detector and the dark-count rate, and it is given by

$$NEP = \frac{h\nu}{\eta} \sqrt{2D},$$

where  $D$  is the dark-count rate,  $\eta$  is the detection efficiency,  $\nu$  is the photon frequency and  $h$  is the Planck's constant.  $NEP$  is measured in  $\text{W Hz}^{-1/2}$ , and it should be as low as possible. However, typical detectors (those not

resolving the number of photons in a pulse) do not measure optical power. Moreover, the timing performance of the detector is not taken into account in this figure of merit, and it does not provide a meaningful relationship between  $D$  and  $\eta$  for QKD experiments. Actually, the contribution of the detectors to the QBER is given by the ratio of the dark-count rate to the detected photon rate. Furthermore, the timing jitter  $\Delta t$  of the detector is usually the limiting factor of the minimum time interval of the bit width, which is related to the maximum clock frequency and consequently the maximum net bit rate. Therefore, a dimensionless figure of merit useful for QKD that takes all of these factors into consideration can be formulated as

$$H = \frac{\eta}{D\Delta t}.$$

For a given wavelength, the higher the value of  $H$ , the better the detector [Hadfield, 2009].

In addition to the mentioned criteria, an ideal detector should be practical. A detector that needs liquid helium or even nitrogen cooling would certainly render commercial development difficult. Unfortunately, the fulfilment of all the above criteria at the same time turns out quite difficult. Due to their high efficiency, low dark-count rates, sub-nanosecond timing resolution and commercial availability, most of the QKD systems built so far [Stucki et al., 2001], [Hiskett et al., 2001], [Ghioni et al., 2003] have used SPADs as single-photon detectors. Three different semiconductor materials are used: silicon, germanium, or indium gallium arsenide, depending on the operation wavelength.

Silicon single-photon avalanche diodes (Si-SPADs) generally exhibit considerably less afterpulsing effects and lower dark-count rates than Ge and InGaAs single-photon avalanche detectors, which also need to be cooled down to cryogenic temperatures. Si-SPADs operate efficiently only at short wavelengths (typically up to  $\sim 1000$  nm). This is one of the two main reasons considered for the selection of an operating wavelength of  $\lambda \sim 850$  nm for the QKD system, as discussed in section 3.3.2. The other reason is its low absorption through the atmosphere. There are several single-photon detector technologies available for use at a wavelength of  $\lambda \sim 850$  nm, some of which are discussed in the following section.

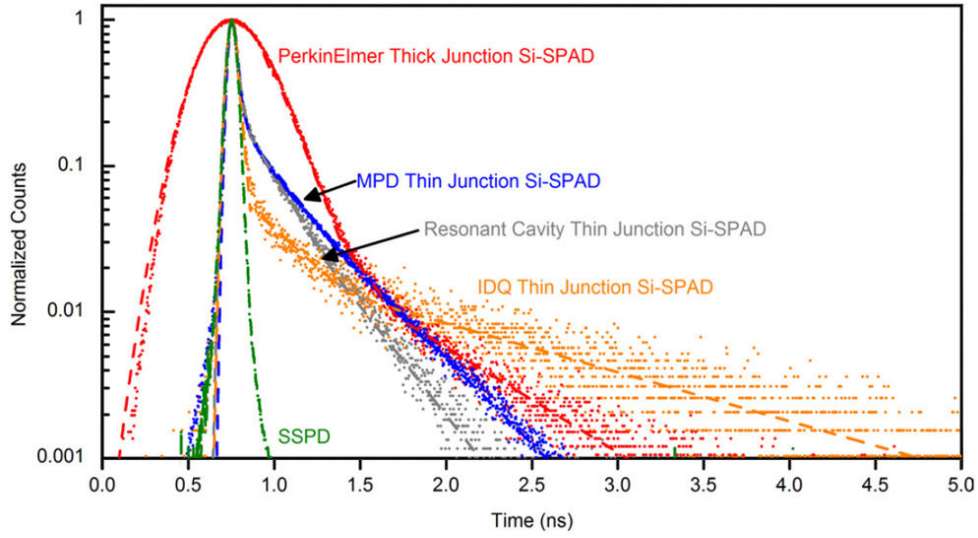
### 5.3.1 Single-photon detectors operating at a wavelength of 850 nm

The timing performance of several single-photon detectors was characterised in a GHz-clocked phase-encoding system described in [Clarke et al., 2011]. A number of previous demonstrations of QKD at a wavelength of 850 nm have used thick-junction Si-SPADs as detectors [Gordon et al., 2004], [Bienfang et al., 2004]. While offering good detection efficiencies of  $\sim 40\%$  at this wavelength, these detectors also exhibit relatively large FWHM timing jitters of  $\sim 400\text{--}500$  ps. Timing jitters of this duration can lead to intersymbol interference at clock rates of  $\sim 1\text{--}2$  GHz as the timing jitter exceeds the clock period, resulting in photon events being recorded in adjacent bit windows. Thin or shallow-junction Si-SPADs have a narrower depletion layer than thick-junction Si-SPADs, and the electric field is concentrated on the surface of the device. Due to this effect, thin-junction Si-SPADs typically have shorter duration timing jitters of  $\text{FWHM} \sim 70$  ps, but can exhibit long tails in their timing profile caused by relatively slow diffusion of photo-generated carriers into the device multiplication region [Dautet et al., 1993]. These diffusion tails (see Figure 5.3) can be characterised by the FWHM, full-width at 10th-maximum (FW10%M) and full-width at 100th-maximum (FW1%M) timing jitters, and are reported numerically in Table 5.1. These thin-junction detectors generally exhibit reduced detection efficiencies of  $<10\%$  at  $\lambda \sim 850$  nm.

**Table 5.1** – Characteristic parameters of specific detectors when used at a wavelength of 850 nm.

Type	Detector	DCR ( $s^{-1}$ )	Detection efficiency (%)	FWHM (ps)	FW10%M (ps)	FW1%M (ps)
Thick-junction Si-SPAD	PerkinElmer	198	42	432	837	1473
Thin-junction Si-SPAD	MPD	200	8.4	71	276	898
	IDQ	15	1.6	63	193	1245
	Resonant cavity	21	18	74	271	913
NbN superconducting nanowire	SSPD	10	10	62	120	196

The detection efficiency of a thin-junction Si-SPAD may be enhanced, without compromising the temporal response and dark-count rate, by the use of



**Figure 5.3** – Normalised instrument responses for the indicated detectors.

a resonant cavity to increase the effective interaction length for absorption of incident photons [Ghioni et al., 2009]. The instrument response of such a detector can be seen in Figure 5.3, where it may be observed that it is comparable with that of a similarly structured thin-junction Si-SPAD from Micro Photon Devices (MPD), which was grown on an all-silicon substrate and did not incorporate a resonant cavity.

In recent years, there has been a great deal of interest in the use of nanowire superconducting single-photon detectors (SSPD) [Takesue et al., 2007], [Collins et al., 2007]. These detectors are based around a thin, narrow strip of a superconducting material, such as niobium nitride (NbN). This NbN strip is biased close to the critical current and cooled to a temperature below the superconducting transition temperature (typically of 3 K). An incident photon creates a resistive hotspot as the current density in specific parts of the nanowire exceeds the critical level, which leads to a readily detectable current pulse. The thin-junction Si-SPADs and the SSPD exhibit comparable FWHM timing jitters. However, compared to the rest of detectors under analysis, the SSPDs have an approximately Gaussian temporal response, as can be seen in Figure 5.3. An SSPD may be operated at a number of different bias currents —as the bias current is increased, the detection efficiency increases but the dark-count rate also increases. In the experiments described in [Clarke et al., 2011], the SSPDs

have a detection efficiency of  $\sim 10\%$  at a wavelength of  $\lambda \sim 850$  nm, which corresponded to a dark-count rate of  $\sim 10$  counts/s. SSPDs have previously been proved at GHz clock rates in various QKD demonstrations [Takesue et al., 2007], [Tanaka et al., 2008].

The detectors characterised in [Clarke et al., 2011] were a PerkinElmer SPCM-AQR-12 thick-junction Si-SPAD with an active-area diameter of  $180\text{ }\mu\text{m}$  [PerkinElmer, 2005], a  $20\text{ }\mu\text{m}$  active-area diameter thin-junction MPD PDM CCTC Si-SPAD [MPD, 2012], a  $50\text{ }\mu\text{m}$  active-area diameter IDQ id100-MMF50 thin-junction CMOS Si-SPAD [IDQ, 2012], an experimental  $20\text{ }\mu\text{m}$  diameter active-area resonant cavity thin-junction Si-SPAD [Ghioni et al., 2009] and a NbN nanowire meander line SSPD with a meander area of  $20\text{ }\mu\text{m} \times 20\text{ }\mu\text{m}$  and a fill factor of 50% [Miki et al., 2008]. The SSPD was operated at a temperature of 3 K in a closed-cycle refrigerator [Radenbaugh, 2004], whereas the rest were peltier-cooled to an operating temperature in the range of  $\sim 230 - 260$  K. The experiments proved that, as a consequence of their lower overall QBER values due to the lower FWHM timing jitters they exhibit, the experimental resonant cavity Si-SPAD and the SSPD gave higher sifted bit rates at a clock frequency of 1 GHz despite having lower detection efficiencies than the PerkinElmer thick-junction Si-SPAD. However, it has been previously shown that the FWHM timing jitter of a PerkinElmer thick-junction Si-SPAD can be reduced by modifying the pulse readout electronics within the detector module [Rech et al., 2006]. This modified circuit reduced the FWHM timing jitter of the detector without affecting the dark-count rate or detection efficiency. The shortest FWHM timing jitter of an unmodified PerkinElmer Si-SPAD described in the literature was 350 ps, which decreased to 200 ps after circuit modification [Restelli et al., 2010]. This improved timing jitter indicates that the modified PerkinElmer thick-junction Si-SPAD can provide secure key exchange rates comparable with the SSPDs and the resonant cavity Si-SPADs.

### 5.3.2 Single-photon avalanche diodes

As already mentioned, due to their high efficiency, low noise, simplicity and commercial availability, Silicon single-photon avalanche diodes have been used

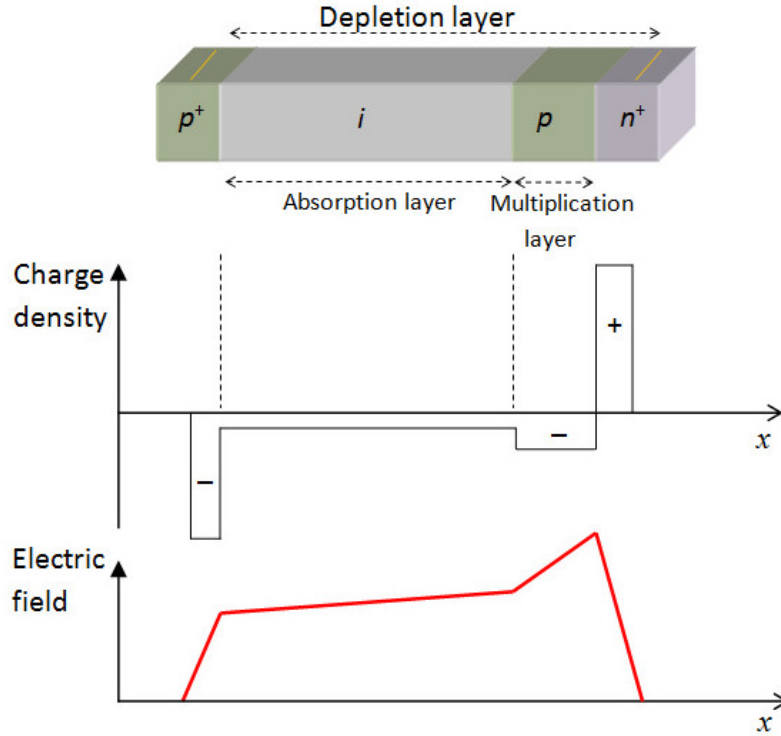
in the QKD system discussed in this thesis. Their structure and principle of operation are described in the following.

Single-photon avalanche diodes are based on an avalanche photodiode (APD) structure. APDs are based on the avalanche breakdown process in semiconductors. This process takes place when an electron-hole pair generated by the absorption of a photon gains sufficient kinetic energy (due to the existence of a high electric field across the device) to ‘release’ further electron-hole pairs via the process of *impact ionisation*. The geometry of an APD should on one hand maximise photon absorption, and on the other hand minimise the generation of localised uncontrolled avalanches being produced by the strong electric field (greater electric-field uniformity can be achieved in a thin region). Both requirements demanded that APDs with separated absorption and multiplication regions were designed, which are known as Separate-Absorption-Multiplication APD (SAM APD) devices. Photons impinging on the detector are absorbed in a large intrinsic region, and then the generated electrons drift across this region towards the region with a stronger electric field. In the multiplication layer they gain enough energy for avalanching to occur. An example of this device is illustrated in Figure 5.4 [Saleh et al., 2007, S18.4].

SPADs are avalanche photodiodes which are reverse-biased beyond their *avalanche breakdown voltage*, what is known as *Geiger mode* operation (see Figure 5.5), leading to an absorbed single photon being able to trigger an electron avalanche. Hence, single photons are able to generate a current large enough to be detected and used by the electronics of the APD.

However, carriers that are generated by photon absorption experience avalanche gain, which triggers a macroscopic breakdown of the diode junction. To control this effect in a practical device the avalanche must be stopped and the equilibrium must be restored in order to enable the detection of the next photon. This is achieved by means of a *quenching* process [Cova et al., 1996]. Three possible quenching circuits can be used: *passive quenching*, *active quenching* and *gated-mode* circuits.

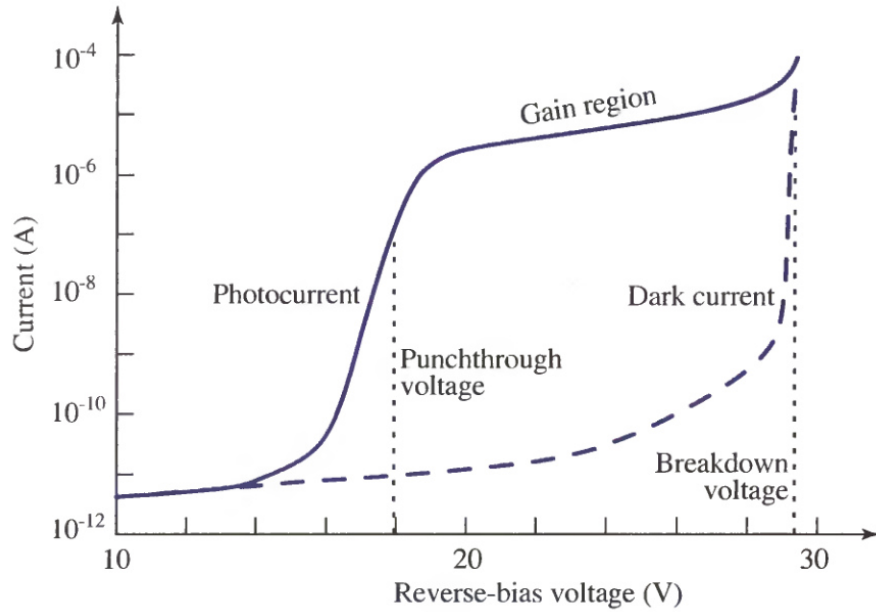
In passive-quenching circuits a large resistor ( $50 - 500 \text{ k}\Omega$ ) is connected in series with the APD. This causes the voltage across the APD to decrease as soon as the avalanche starts [Brown et al., 1986]. When the voltage is below the breakdown voltage the avalanche stops and the diode recharges. The recovery



**Figure 5.4** – Schematic of a *reach-through* avalanche photodiode structure (after [Saleh et al., 2007]). The region  $i$  is very lightly doped. The regions  $p^+$  and  $n^+$  are heavily doped. The electric field reaches a maximum in the multiplication layer. Photon absorption occurs in the wide intrinsic region. Electrons drift through the intrinsic region into a thin  $p - n^+$  junction, where they experience a sufficiently strong electric field to cause avalanching. The device is called a “reach-through” device since, with the application of sufficient reverse bias, the depletion region reaches through the intrinsic material to the  $p^+$  area and maximises the absorption volume.

time of the diode depends on its capacitance and on the value of the resistor. Maximum count rates between a few hundred kilohertz and a few megahertz can be obtained.

In active-quenching circuits the bias voltage is actively forced below the breakdown voltage immediately after the leading edge of the avalanche current is detected [Brown et al., 1987]. Since this permits shorter dead times (tens of nanoseconds) than in passive quenching, count rates up to tens of megahertz can be obtained.



**Figure 5.5** – Typical trace of the photocurrent of an APD. Internal gain is achieved when the APD is biased above the avalanche breakdown voltage.

In gated-mode operation the bias voltage is maintained below the breakdown voltage and it is raised above it only for a few nanoseconds when a photon arrival is expected. This reduces efficiently the dark-count rate due to trapping effects. If the detector is gated off for a period sufficiently long enabling all the carriers to release, trapping effects contribution can be reduced noticeably [Levine et al., 1984]. This mode of operation is commonly used in quantum key distribution with WCP, where the incoming photons are expected within a known arrival time. Prior timing information is then needed and it should be suitably characterised.

### 5.3.3 PerkinElmer Single Photon Counting Module

The QKD system investigated in this thesis uses PerkinElmer Single Photon Counting Modules (SPCM) AQR 12 [PerkinElmer, 2005]. The SPCM-AQR-12 is a self-contained device, which uses a thick-junction Si-SPAD with an active area of  $180 \mu\text{m}$  diameter and a wavelength detection range from 400 to 1060 nm. It also contains an active quenching circuit (AQC) and a temperature



controller. The datasheet of the PerkinElmer module [PerkinElmer, 2005] quotes a maximum output count rate of 15 Mcounts/s before saturation, a detection efficiency of approximately 45% at 830 nm, a maximum dark-count rate of 500 counts/s, a typical dead time of 50 ns between pulses, and an afterpulsing probability of 0.5%.

Four PerkinElmer SPCMs, labelled SPAD 1, SPAD 2, SPAD 3 and SPAD 4, were characterised in terms of detection efficiency and dark-count rate (see Table 5.2). For that purpose a VCSEL emitting at a wavelength of 847.7 nm was modulated at a frequency of 25 MHz, and its optical output was attenuated up to a 0.1 mean photon number per pulse so that a rate of 2.5 Mcounts/s reached the detectors. The counts at the output of the SPADs were measured with a photon counter (SR400).

The ratio of the dark-count rate  $D$  to the detection efficiency  $\eta$  was calculated. This figure of merit pointed to SPAD 1 and SPAD 2 as the better detectors. However, to take into account the timing jitter of the detectors, an additional experiment was performed to measure the QBER of the transmission of a bit sequence. It turned out that, under the same conditions, the detectors that provided the lower QBERs were SPAD 1 and SPAD 3, hence they were the detectors selected for the experiments discussed in chapter 6.

**Table 5.2** – Comparison of several relevant features for four PerkinElmer SPCMs.

Detector	Detection efficiency $\eta(\%)$	Dark-count rate $D(\text{counts/s})$	$D/\eta$
SPAD 1	29.2	170	5.82
SPAD 2	26.2	140	5.34
SPAD 3	35.5	250	7.04
SPAD 4	31.6	400	12.66

## 5.4 Time Interval Analyser

The timestamp card used to record the time of arrival of each detected photon is a GT658PCI from GuideTech. It consists of an ultra-fast, DC–400 MHz Time Interval Analyser (TIA) with a timing resolution of 75 ps. TIAs are

super high-speed time and frequency measurement instruments, the fast measurement rate of which, compared to traditional time interval counters, provides new capability to analyse dynamic changes in frequency or time intervals [Guidetech, 2009].

Basically, time interval analysers log the time of occurrence of events at their data inputs. Events are defined as a signal voltage crossing a specified threshold in the positive or negative direction. These “time-tags” of the positive or negative edges are logged into memory along with the total count of edges received.

The GT658 card has two main input channels, A and B, where the outputs of the two SPADs of the receiver are connected to. It also has an external-clock input (EXT CLK) for a user-supplied 10 MHz reference, to be used instead of the on-board 10 MHz timebase. This external 10 MHz reference was given by the synchronisation signal at  $\lambda \sim 1550$  nm.

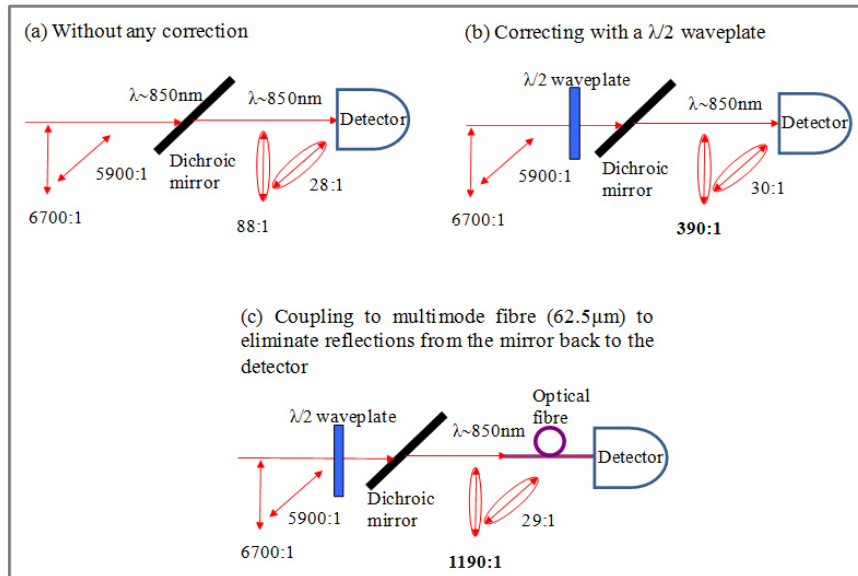
The I/O block of the board is composed of four comparators that “square” the input signals. Each comparator’s output is a logic high whenever the positive input voltage is greater than the negative input, and a logic low otherwise. The analog input signals of the TIA are applied to the positive inputs of the comparators, and a programmable voltage is applied to the negative inputs. This programmable voltage dictates the voltage point on the signal in which an event will be captured. Each of the two main channels (A and B), and the EXT CLK input, have separate threshold settings.

The LabVIEW user interface supplied with the TIA allows enabling each data channel separately, and setting the respective input impedances ( $50\ \Omega$  or  $1\ \text{M}\Omega$ ) and threshold voltages also independently. Some modifications were applied to the software so that after each measurement (key exchange) was performed, the software provided the number of events received per second and the lists of arrival times detected in each data input.

## 5.5 Analysis and correction of the polarisation extinction ratio

To minimise the fraction of photons, the polarisation of which is erroneously detected (thus increasing the error rate), the polarisation extinction ratio of the quantum states must be characterised through the optics of the receiver in order to allow identifying the optical elements contributing to polarisation degradation and hence to apply the necessary measures to correct the linearity of the polarisation states.

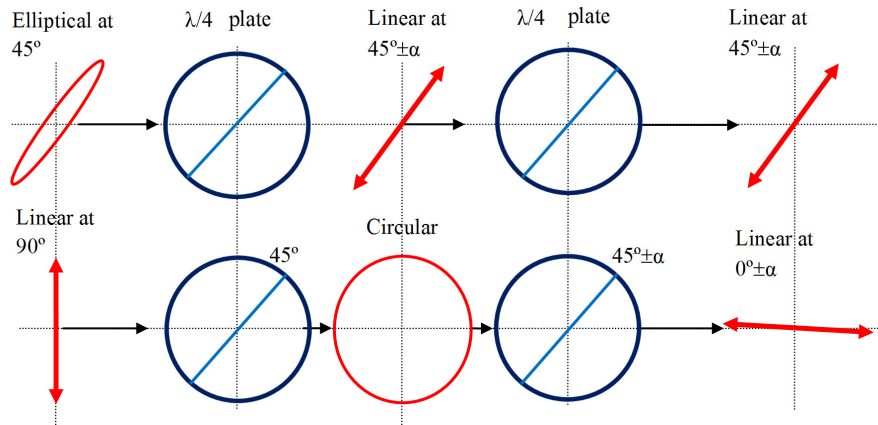
Therefore, a thorough analysis of the PER through the optical receiver module was performed. It was observed that the dichroic or pump mirror used to discriminate the synchronisation signal at  $\lambda \sim 1550$  nm and the data signal at  $\lambda \sim 850$  nm, was the component that deteriorated the linearity of the polarisation states the most. To minimise the effect of the dichroic mirror on the polarisation the ‘vertical state’ was aligned with one of the axes of the dichroic mirror by using a half-wave plate (see Figure 5.2). The ‘diagonal state’, at  $45^\circ$  from the ‘vertical state’, remained between the two axes of the dichroic mirror, and hence its polarisation became elliptical.



**Figure 5.6** – Polarisation degradation after the dichroic mirror at  $\lambda \sim 850$  nm. The PER of the vertical quantum state was analysed and corrected by using a  $\lambda/2$  waveplate.

Figure 5.6 shows the worsening of the PER of both states after passing through the dichroic mirror (Figure 5.6-a), and how the PER of the ‘vertical state’ improved when the half-wave plate was used (Figure 5.6-b). The coupling of the signal into a multimode optical fibre with a diameter of  $62.5\ \mu\text{m}$  filtered the reflections from the mirror back to the detector, thus further improving the PER of the ‘vertical state’ (Figure 5.6-c). The ‘diagonal state’ did not improve with the fibre coupling due to its low PER.

To recover the linearity of the ‘diagonal state’ two quarter-wave plates were used. The process by which two quarter-wave plates improve the PER of one polarisation state without altering the other state at  $45^\circ$  is illustrated in Figure 5.7. The first quarter-wave plate is oriented so that the ‘diagonal state’ becomes as linear as possible. On the other hand, as the ‘vertical state’ is incident on the first quarter-wave plate at  $\sim 45^\circ$  to the optical axis of the plate, its polarisation becomes almost circular after passing through it. The second quarter-wave plate is then used to recover the linearity of the vertical state, since incident circularly polarized light is changed to linearly polarised light.



**Figure 5.7** – Effect of two consecutive quarter-wave plates on the polarisation of two non-orthogonal states.  $\alpha$  is the ellipticity degree of the incoming diagonal polarisation state.

As already explained in section 5.2, each polariser is oriented at  $45^\circ$  to the polarisation state to be detected in its corresponding channel, that is, orthogonally to the polarisation to be extinguished in that channel. Therefore ‘channel 0’ blocked the polarisation state of the ‘1’s, represented by the

diagonal state; and ‘channel 1’ blocked the ‘0’s, or vertical states. Efficiently blocking these states is crucial to keep the error rate low, and the less linear they are, the worse the blocking is. Therefore, improving the PER of the ‘blocked states’, especially the ‘diagonal state’ in ‘channel 0’ (as it was the less linear state) was essential. This was done with the two  $\lambda/4$  plates in ‘channel 0’, as explained above.

Figure 5.8 shows the PER values of the two polarisation states in the transmission and reflexion channels of the receiver, ch0 and ch1 in the figure. As discussed above, it can be seen how the use of the half-wave plate improves the PER of the ‘vertical state’ in both channels, and how the two quarter-wave plates in channel ‘0’ improve the PER of the ‘diagonal state’ in this channel. This reduces the polarisation-induced QBER, i.e., the contribution to the error rate due to polarisation leakage.

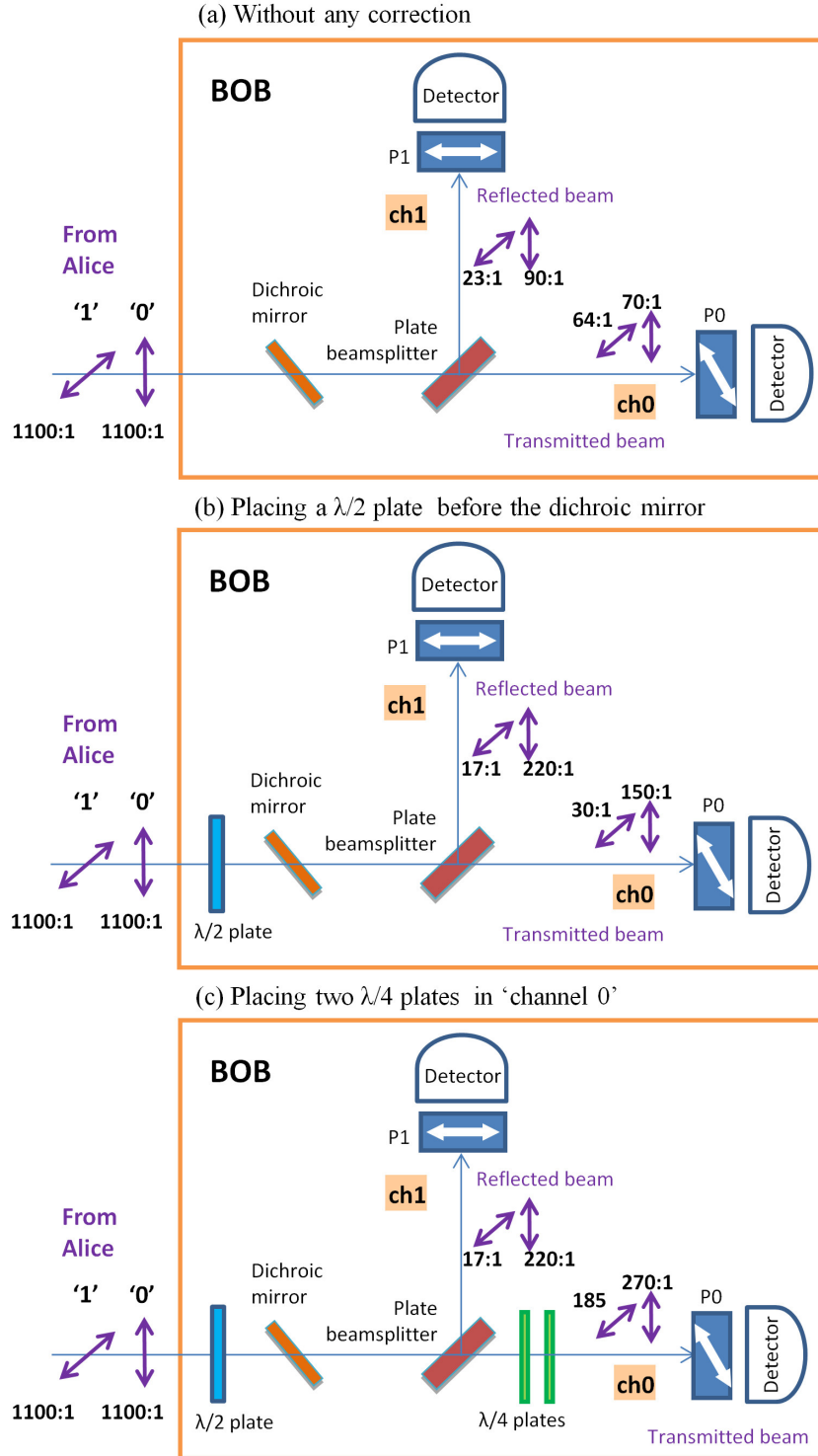
## 5.6 Receiver loss

The overall optical loss of the receiver was characterised through measuring the contribution of each component in order to estimate the count rate expected at the receiver for each emission rate at the transmitter. The loss of each of Bob’s components at a wavelength of 850 nm is summarized in Table 5.3.

**Table 5.3** – Total loss of the receiver and optical loss of each optical component.

Component	Insertion loss (dB)
Telescope	4.43
$\lambda/2$ plate	0.2
Dichroic mirror	0.16
Interference filter	1.6
Beamsplitter plate	0.05
Polariser	1.46
Optical fibre ( $\varnothing = 62.5 \mu\text{m}$ )	0.7
<b>Total loss</b>	<b>8.6</b>

The highest loss of the system (4.43 dB or 64% loss) is due to the anti-reflection coating of the Schmidt-Cassegrain telescope, which is designed to



**Figure 5.8** – PER of the non-orthogonal polarisation states at the receiver in three cases: (a) without applying any polarisation-correcting measure, (b) improving the vertical state in ch1 by using a  $\lambda/2$  plate, and (c) improving the diagonal state in ch0 by using two  $\lambda/4$  plates. P0 and P1 are two high extinction polarisers.

enhance the transmission of the telescope at the visible range, as shown in Figure 5.9, thus decreasing other wavelength ranges. Quotes for the transmission at  $\lambda \sim 850$  nm were not available, but it can be estimated from the transmission curves of the Meade telescope that if the tendency of the “Meade Ultra-High Transmission Coatings” curve is maintained, then the transmission at a wavelength of 850 nm may agree with the measured telescope loss (4.43 dB loss  $\equiv \sim 36\%$  transmission).

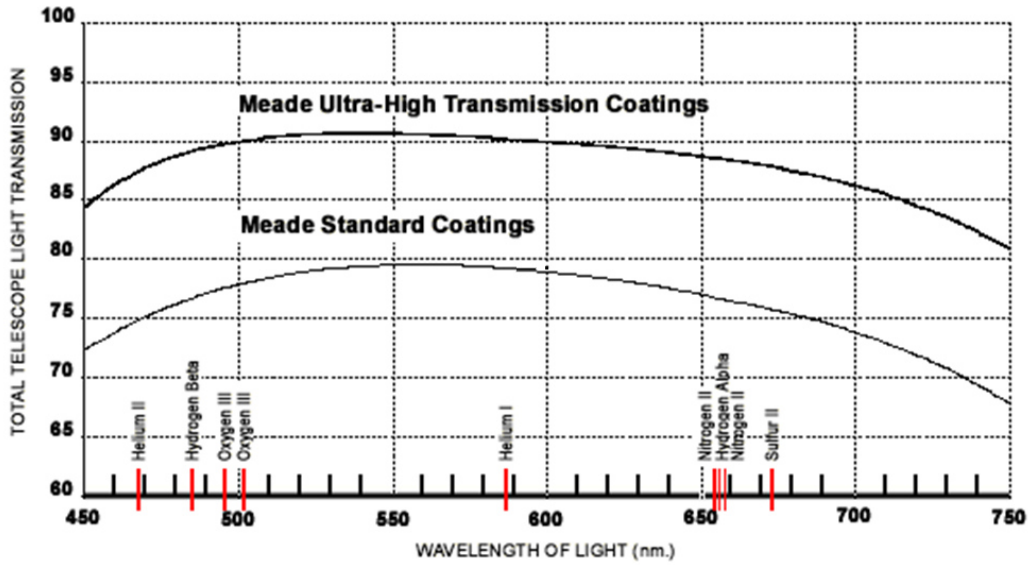


Figure 5.9 – Transmission curves of the Meade telescope.

The total efficiency of the QKD receiver,  $\eta_{receiver}$ , can then be calculated as

$$\eta_{receiver} = \eta_{opt} \times \eta_{protocol} \times \eta_{spad},$$

where  $\eta_{opt}$  is the transmission of the optical module including the telescope,  $\eta_{protocol}$  is the efficiency of the B92 protocol, and  $\eta_{spad}$  is the detectors efficiency. The optical loss in Bob module (8.6 dB  $\equiv 0.14$  transmission), the efficiency of the B92 protocol (0.25), and the detection efficiency of the SPADs ( $\sim 0.32$ ), yield a total receiver efficiency of  $\sim 0.01$ . Therefore, knowing the count rate emitted by Alice it is possible to calculate the expected count rate at Bob. For example, if the emitter sends a sequence to the receiver at a frequency of 1 GHz with a mean photon number per pulse  $\mu$  of 0.1, a photon rate of 100 Mcounts/s would be emitted, and a count rate of  $\sim 1$  Mcounts/s would be

detected in the receiver, without taking into account the transmission loss of the quantum channel ( $\sim 2$  dB/km).

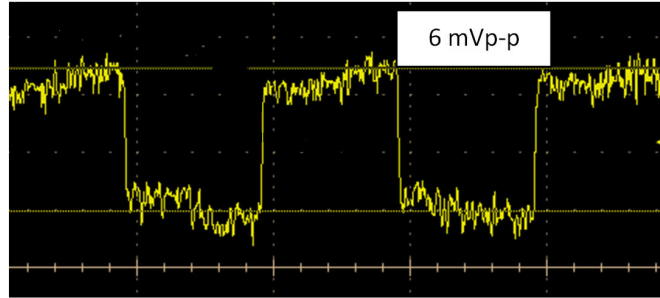
### 5.7 Detection of the synchronisation signal at the receiver

As already mentioned, the signal at  $\lambda \sim 1550$  nm carries the 10 MHz reference (synchronous with the data signal at  $\lambda \sim 850$  nm), which is connected to the external-clock input of the time interval analyser. The minimum voltage level needed at the external-clock input of the TIA was measured to be 140 mV peak-to-peak with 1 k $\Omega$  input impedance. The loss of the  $\lambda \sim 1550$  nm signal from emitter to receiver was then characterised for a 30 m link to verify whether the power at the receiver would be enough for the TIA to operate. The optical power from the pigtailed fibre of the  $\lambda \sim 1550$  nm laser at the emitter at its maximum modulation current was  $\sim 550$   $\mu$ W, while the received power in Bob at the entrance of the  $\lambda \sim 1550$  nm photodetector was  $\sim 120$   $\mu$ W, which meant the synchronisation signal experienced a loss from the emitter to receiver of 6.6 dB. A large part of the loss was due to the coating of the receiver telescope. As the InGaAs photodetector (Thorlabs DET01CFC) used to transform the optical synchronisation signal into an electrical signal had a photo sensitivity of 0.95 A/W, the voltage at the external-clock input of the TIA was 114 mV (with 1 k $\Omega$  input impedance), which was insufficient for the operation of the card.

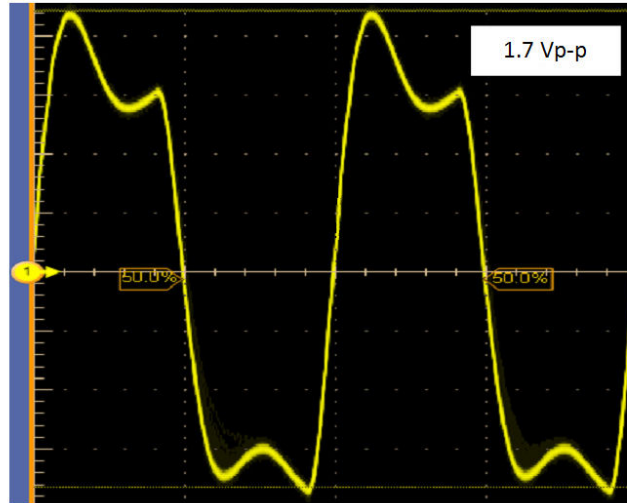
Consequently, a trans-impedance amplifier was designed and implemented to increase the voltage level of the synchronisation signal. This amplifier had a gain of  $-15 \cdot 10^3$  V/A, a bandwidth of 60 MHz, and was capable of detecting powers as low as 10  $\mu$ W. Using this amplifier a  $\sim 1.7$  V synchronisation signal was viewed in the oscilloscope at the receiver (with a load of 1 k $\Omega$ ), which corresponded to an optical power of  $\sim 119.3$   $\mu$ W. This level of the synchronisation signal was more than sufficient for the correct operation of the external-clock input of the timestamp card.

The synchronisation signal was measured in an oscilloscope at the input and output of the trans-impedance amplifier (represented in Figures 5.10 and 5.11).





**Figure 5.10** – Screen capture of the synchronisation signal measured at the output of the InGaAs photodetector. The input impedance of the oscilloscope was set to  $50\ \Omega$ .



**Figure 5.11** – Screen capture of the synchronisation signal measured at the output of the trans-impedance amplifier. The input impedance of the oscilloscope was set to  $1\ \text{M}\Omega$ .

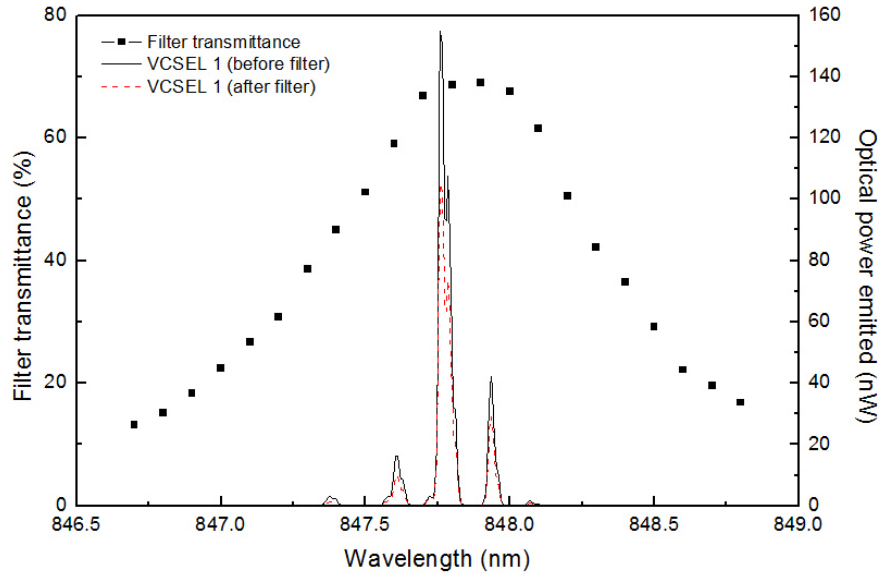
The figures show that the signal amplification was obtained at the expense of an increment of its rise and fall times. The InGaAs photodetector has a bandwidth of 1.2 GHz and provides an output signal with low rise and fall times. However, as mentioned above, the voltage of the signal was not high enough for the TIA to operate. The current at the output of the photodetector was  $\sim 114\ \mu\text{A}$  (for an optical power input of  $\sim 120\ \mu\text{W}$ ) which, measured in the oscilloscope with a load of  $50\ \Omega$ , resulted in a voltage amplitude of 6 mV. After the trans-impedance amplifier the signal reached 1.7 V.

## 5.8 Filtering and shielding from background light

One of the most critical parts of the QKD system is the filtering of solar background radiation, as it is essential for the system operation in daylight conditions. With the aim of reducing the amount of background light that may be collected by the receiver, and therefore increasing the signal-to-noise ratio, a combination of spectral and spatial filtering is used.

The spectral filtering is performed by a 1 nm FWHM interference filter (IF) centred at a wavelength of  $\sim 848$  nm. The filter was placed between the dichroic mirror and the beamsplitter plate in the receiver module (see Figure 5.2). The spectral transmission band of the filter was characterised by using a spectrometer. As shown in Figure 5.12, the interference filter has a maximum transmission of  $\eta_{filter} \sim 0.7$  at  $\lambda \sim 848$  nm. The figure also shows the optical power emitted by VCSEL1 at different wavelengths, and how it is attenuated after passing through the filter by about 1.7 dB (dashed line). This filter lowered the contribution of the solar background leaked in the receiver by more than 30 dB. This was a major factor to achieve daylight operation with low error rates at a distance of 300 m, as it will be discussed in chapter 6.

Figure 5.12 suggests that a narrower filter could be used for a further reduction of the background radiation (for instance of 0.2 nm FWHM), since the central mode of the VCSEL has a spectral width of  $\sim 0.1$  nm. However, using a very narrow band filter places a demanding requirement upon the emitting source to stay within the transmission band of the filter. The drivers of the VCSELs contain an automatic power control that adjusts the laser bias current to maintain an average optical power output over temperature and changing laser properties. Moreover, in section 3.3.5 it was shown that the spectrum of the VCSELs shifts with the bias current by  $\sim 76$  pm/mA in the range of bias currents close to the minimum bias. Therefore, if a  $< 1$  nm wide interference filter was to be used, a monitored temperature control of the kind of a Peltier cooler would be required at the emitter to ensure the matching of the filter and the lasers emission wavelength along the time. This option was considered but later discarded due to the difficulty of attaching such a cooler to the VCSELs, since these were soldered onto an electronic board. Facing this situation single-mode VCSELs should have been used to reduce the spectral



**Figure 5.12** – Transmittance of the interference filter (left-hand axis) and optical power emitted by VCSEL1 (right-hand axis) against wavelength. The calculated optical power after passing through the filter is plotted in dashed style.

information leakage to an eavesdropper. Unfortunately the lack of availability of high-bandwidth single-mode VCSELs with the desired characteristics made this option were abandoned.

The spatial filtering of background radiation is accomplished by the optical fibres that are used to convey the signals at  $\lambda \sim 850$  nm into the SPADs. A good compromise for the diameter of these fibres must be found, as small diameters improve the filtering of background radiation, albeit at the expense of a higher signal loss. When no automatic tracking is implemented, if the diameter of the fibres is too small, the system becomes more vulnerable to effects such as the beam wander caused by turbulences in the transmission channel. The fibres used in the system discussed in this thesis have a core diameter of  $62.5 \mu\text{m}$ , giving the receiver a restricted field of view but allowing a good coupling of the signal.

In addition to the background radiation that is collected by the receiver telescope, stray background light at the receiver's location may couple into the optics and increase the error rate. To prevent this, Bob's optics module was covered with light blackout fabric (see Figure 5.13). The isolation of emitter

and receiver from stray background radiation reduced the amount of stray light that was coupled into the receiver by several orders of magnitude, which also greatly contributed to enabling full bright daylight operation.



**Figure 5.13** – Picture of the receiver covered with the blackout fabric.

Other systems, as well as spectral and spatial filtering, use temporal filtering to render the background tractable [Hughes et al., 2002b], [Peloso et al., 2009]. This technique consists in the emission from Alice of a short bright timing pulse that is launched towards the receiver preceding each single-photon pulse. At Bob, the timing pulse is detected by a photodiode and sets a timing window in which a data photon is expected, that is, the bright signal allows Bob to gate his single-photon detectors so that only photons that occur in that narrow timing window are detected. The SPADs used in the QKD system investigated in this thesis cannot be gated at GHz clock frequencies (their maximum gating frequency is  $\sim 20$  MHz), and therefore this method of temporal filtering was not implemented. Software filtering on the other hand, can always be implemented by rejecting events that fall outside selected time windows superimposed over each bit width. However, although both of the previous techniques are useful to improve the signal-to-noise ratio, they limit the overall bit rate of the QKD system, and therefore they were not implemented. In the system discussed in this thesis the spectral and the spatial filtering, along with the light-shielding

of the system, were enough to permit daylight operation with high secret key exchange rates.

## 5.9 Conclusions

In this chapter the configuration and performance of the experimental QKD receiver has been presented. Firstly, a full description of the optics module, where the polarisation analysis of the received photons according to the B92 protocol takes place, has been given. Then the choice of SPADs as the detectors of the system has been discussed and their general features have been compared to other single-photon detectors. Their high efficiency, low noise, practicality and commercial availability, made them the most suitable option. The characterisation of four Si-SPADs devices in terms of their detection efficiency, dark-count rate and QBER has also been described, highlighting the two SPADs with the best performance. The timestamp card or Time Interval Analyser used to record the time of arrival of the detected photons has also been described.

Moreover the characterisation of the polarisation extinction ratio of the non-orthogonal quantum states received by Bob has been presented. A half-wave plate and two quarter-wave plates were utilised in the receiver to correct the ellipticity of the polarisation states, caused mainly by the birefringence of the dichroic mirror.

The overall optical loss of the receiver and the detailed contribution of each component have been measured. The total efficiency of the receiver has been characterised, so that predictions on the expected count rate at the receiver for a determined output bit rate at the transmitter can be done.

The InGaAs photodetector used for the detection of the synchronisation signal and the trans-impedance amplifier required to enhance the voltage level given by this photodetector have been also described. The trans-impedance amplifier increased the amplitude of the synchronisation signal so that the requirement on the voltage level at the EXT CLK input of the time interval analyser was sufficiently fulfilled.

Finally, the spectral and spatial filtering and the light-tight isolation of the receiver by means of blackout fabric have been described as the measures

taken to reduce the background radiation that may couple into the receiver. The 1 nm FWHM interference filter, centred at the lasers emission wavelength, reduced the background by 30 dB over what would be experienced by a bare detector. Moreover, the spatial filtering carried out by optical fibres with a core diameter of  $62.5\text{ }\mu\text{m}$ , gave the receiver a restricted field of view. This provided several orders of magnitude reduction in the background radiation that was collected by the receiver over what would be expected with the acceptance angle of a detector without the fibre. The above mentioned measures taken for the filtering of the background radiation were sufficient to permit daylight operation at high transmission rates.

## Chapter 6

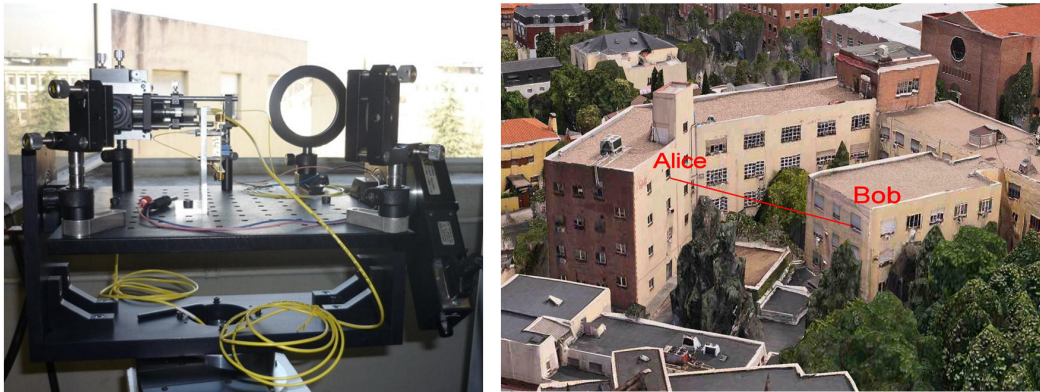
# Experimental results for two optical links

The final goal of a QKD system is the generation of a secret key shared by Alice and Bob. In previous chapters the design of sender and receiver, and a detailed characterisation of each station were described. The techniques necessary for the correct operation of the system, such as background filtering and timing synchronisation were also discussed. In this chapter the characterisation of the entire free-space quantum key distribution system is presented. In addition, the calculation of the QBER and secret key rate are also described. The experimental results presented in this chapter were obtained for two optical links at different distance: 30 and 300 m. Firstly, transmitter and receiver were placed 30 meters apart in two different laboratories of the same institute that held a line of sight. Then, the transmitter was taken to a different location at a distance of 300 meters from the receiver. The configuration of the QKD system and the techniques carried out to align both stations are discussed for both optical links. Several experiments were performed for these two links with the aim of establishing the system's

optimum clock frequency, the optimum mean photon number per pulse  $\mu$ , the influence of background radiation, and the system's stability and robustness to misalignment. In the following, the characterisation of the system's performance and several important parameters such as the QBER, sifted and secure bit rate, and background rate, are presented and discussed for the two mentioned optical links. The results obtained from the measurements carried out for the characterisation of the QKD system at 300 m have been deeply discussed in [García-Martínez et al., 2013].

## 6.1 Setup and location of the QKD links

Several experiments were performed to characterise the QKD system for the mentioned two links of different distance in downtown Madrid. Firstly, sender and receiver were located  $\sim 30$  m apart, specifically in two laboratories with line of sight at the fourth floor of the Information Security Institute of the Spanish National Research Council (CSIC). In Figure 6.1 a picture of the view from the transmitter's side and an aerial view of the link are shown.



**Figure 6.1** – View from the transmitter's side to the receiver (left) and aerial view of the 30 meter link (right).

After the experiments at 30 meters were finished, the transmitter was moved to a different building at a distance of  $\sim 300$  m from the receiver—concretely to the sixth floor of the Institute of Agricultural Sciences also



belonging to CSIC— with the aim of testing the system at a longer distance. The receiver stayed in the fourth floor of the Information Security Institute, but was moved to a different laboratory that held line of sight to the new location of the transmitter. Figure 6.2 shows the view from the transmitter’s side to the receiver and an aerial view of the link.



**Figure 6.2** – View from the transmitter’s side to the receiver (left) and aerial view of the 300 meter link (right).

The alignment procedure between transmitter and receiver consisted in both a coarse and a fine alignment technique. For the coarse alignment Bob’s location was imaged at the focal plane of Alice telescope and a visible laser at  $\lambda \sim 650$  nm was connected to one of the  $\lambda \sim 850$  nm channels to visualise the focal point. This focal point was then aligned with the image of the receiver’s approximate position (the image of the receiver’s window) by using the DC motors at Alice.

Then another  $\lambda \sim 650$  nm laser was connected to a fibre-optic collimator that was mounted in parallel with the data and synchronisation channels in the transmitter. Once the red spot of this laser was seen at the receiver, it was taken —by moving Alice’s DC motors— to a pre-established position at the aperture of the receiver telescope to maximise the signal reception. Then, a fine alignment was performed by fine tweaking Alice’s and Bob’s motors, as well as the  $xyz$  mounts holding the optical fibres of Bob module, through maximising the detected optical power of the  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm beams at the output of their respective optical fibres (see subsection 4.2.4).

For the 30 meter link the laser at  $\lambda \sim 650$  nm was launched directly through the synchronisation channel at  $\lambda \sim 1550$  nm in Alice, and hence there was

no need of using a parallel beam, as the  $\lambda \sim 650$  nm beam did not diverge much at such distance. The alignment techniques were similar to those above explained for the 300 m link, although with a simpler coarse pointing since the distance was considerably smaller. The QKD system was perfectly aligned when the detected signals at  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm agreed with the previously characterised losses of the channel and receiver at both wavelengths (see subsections 4.1.3 and 5.6).

## 6.2 The key exchange protocol

As already mentioned in subsection 2.2.3, the QKD system investigated in this thesis implements the B92 protocol using two non-orthogonal linear polarisation states of single photons, vertically and diagonally (at  $45^\circ$ ) polarised, associated with the bit values ‘0’ and ‘1’ respectively.

The protocol starts with Alice sending a random string of photons polarised in two linear states, which encrypt the two binary values. Bob performs measurements on the received qubits with either of two polarisers (see section 5.2 and Figure 5.2). The polariser of each channel is oriented to block the unwanted polarisation state in that channel. Under these measurement scheme Bob can discriminate unambiguously the two non-orthogonal states at the expense of some loss [Clarke et al., 2001]. Hence, as opposed to the BB84, there is no need for reconciliation of basis sets between Alice and Bob, and therefore the string of bits measured by Bob is directly the sifted key.

A short ‘known sequence’, i.e., a publicly broadcasted sequence, is sent by Alice at the beginning of every transmission. This sequence is used by Bob to identify the beginning of his sifted key. Bob then sends Alice the bit positions where he detected a photon (without revealing the bit values), and Alice generates her sifted key from this information.

In the next step of the protocol Alice and Bob compute the QBER, which will be explained in the following subsection. Error correction and privacy amplification are the two last steps in a QKD protocol to extract the final secret key (described in subsection 2.2.4). The calculation of the final secret key rate from the QBER and the sifted bit rate will be discussed in subsection 6.2.2.

### 6.2.1 Calculation of the QBER

As already mentioned, to test for eavesdropping Alice randomly chooses a fraction of bits of her sifted key as test events, and publicly broadcasts their position and binary value. Bob then compute the QBER of these test events as the ratio of wrong events (those for which Alice and Bob's bit values disagree) to the total number of test events.

The calculation of the QBER is performed in a MATLAB routine as explained in the following. This routine makes use of the photon arrival times, which have been previously logged by the timestamp card in Bob. These time-tags are recorded separately for the photons detected as '1' and those detected as '0' by using a program in LabVIEW, which provides the number of events received per second ( $R_{sifted}$ ) and the lists of event times at each data input of the card (one input for the '1's and other input for the '0's). Then, both lists of time-tags are used by Bob in his MATLAB routine to build his sifted sequence, since he knows the bit period and the length of the sequence sent by Alice. The 'known sequence' that Alice sends at the beginning of her transmission is then used by Bob to correct the delay between his and Alice's sequence by using the cross correlation function. Then Bob calculates the QBER using Eq. 2.3 for the test events announced by Alice, and a fine correction of the delay is carried out by finding the time shift that results in the minimum QBER. Finally, Bob indicates Alice the bit positions where he detected a photon. Alice maintains the bits corresponding to these positions sent by Bob and discard the rest to generate her sifted key. Notice that Bob only reveals his bit values of the test events so that Alice can also compute the QBER, but the rest of bits of his sequence (his sifted key) remain undisclosed.

### 6.2.2 Estimation of the secret key rate

To distil a secret key from Alice and Bob's sifted sequences error correction and privacy amplification classical protocols need to be performed. The secret key rate was inferred from a security proof considering the worst case scenario where Eve performs two types of attacks on the channel simultaneously: the *unambiguous state discrimination (USD)* attack [Dušek et al., 2006] and the

*photon number splitting (PNS)* attack [Huttner et al., 1995], [Brassard et al., 2000], discussed in subsection 2.4.3.

All information that Eve shares with Alice by performing these attacks,  $I_{AE}$ , needs to be subtracted from Alice and Bob's sifted sequences to generate the final secret key. It is known that the B92 protocol is vulnerable to the *USD with a lossless channel* attack, whereby Eve can gain 100% of the key if the loss of the channel is  $\geq 71\%$  [Tamaki et al., 2003]. If the loss of the transmission channel is lower, Alice and Bob can distil a secret key, albeit at the cost of discarding the information gained by Eve through privacy amplification. In the experiments at 300 m the loss of the link is 13.2%, thus allowing an eavesdropper to intercept and perform a USD attack to 18.7% of the photons sent by Alice without being detected. If Eve attacks a higher percentage than this, she will generate a loss that she will not be able to compensate for. By performing a USD attack to 18.7% of the photons transmitted by Alice, Eve obtains 29.3% of them unambiguously [Clarke et al., 2001], which corresponds to 5.5% of the emitted photons, and resends them to Bob. The remaining attacked photons, 13.2%, are detected ambiguously, and thus Eve blocks them not to increase the error rate. Eve remains undetected because she replaces the channel by a lossless one and sends only the photons she detected deterministically, thus not increasing the error rate in Bob's measurements. In the case of the experiments at 30 m, the loss of the quantum channel is 1.4%, and the percentage of photons that Eve can attack without being detected is 1.98%. Therefore she obtains unambiguously 0.58% of the photons emitted by Alice.

In addition, it has been considered that Eve simultaneously performs a PNS attack to all the multi-photon pulses transmitted by Alice. The security of QKD systems with weak coherent pulses has been studied in [Gottesman et al., 2004]. Their investigations prove that, even if Alice has an imperfect source, a secure final key can still be distilled if one knows an upper bound of the bits received by Bob that may have leaked all of their signal information to an eavesdropper without introducing any error. The information shared by Alice and Eve is then given by

$$I_{AEtotal} = I_{AE(USD)} + I_{AE(PNS)} , \quad (6.1)$$

where  $I_{AE(USD)}$  is the information shared by Alice and Eve, assuming Eve performs the above mentioned USD attack, and is given by [Clarke et al., 2001]

$$I_{AE(USD)} = p_{AE}(1 - \cos \theta) , \quad (6.2)$$

$\theta$  being the relative angle between the polarisation quantum states (typically  $45^\circ$ ), and  $p_{AE}$  the percentage of photons sent by Alice that Eve can attack without being detected, which depends on the loss of the quantum channel as above discussed.  $I_{AE(PNS)}$  is the information shared by Alice and Eve assuming a PNS attack is taking place, and is given by

$$I_{AE(PNS)} = \frac{p_{multi}}{p_{exp}} = \frac{1 - (1 + \mu)\exp(-\mu)}{1 - \exp(-\tau\mu)} , \quad (6.3)$$

$p_{multi}$  being the probability that a multi-photon pulse is emitted by Alice,  $p_{exp}$  the probability for a non-empty pulse being detected by Bob,  $\mu$  the average photon number per pulse, and  $\tau$  the transmittance of the channel and receiver combined. Therefore the final secret key rate or net bit rate ( $R_{net}$ ) per second is given by

$$R_{net} = R_{sifted} \left[ (1 - I_{AEtotal}) - f(e)H_2(e) - (1 - I_{AEtotal})H_2\left(\frac{e}{1 - I_{AEtotal}}\right) \right] , \quad (6.4)$$

where  $e$  is the QBER computed by Alice and Bob,  $f(e)$  is the efficiency of the error correction process (which has been assumed to be 1.2 [Martínez-Mateo et al., 2010]), and  $H_2$  is the binary entropy function. Therefore to guarantee security, the sifted key rate ( $R_{sifted}$ ) is reduced by  $f(e)H_2(e)$  after error correction and by  $I_{AEtotal} + (1 - I_{AEtotal})H_2(e/(1 - I_{AEtotal}))$  in privacy amplification.

### 6.3 Experimental results

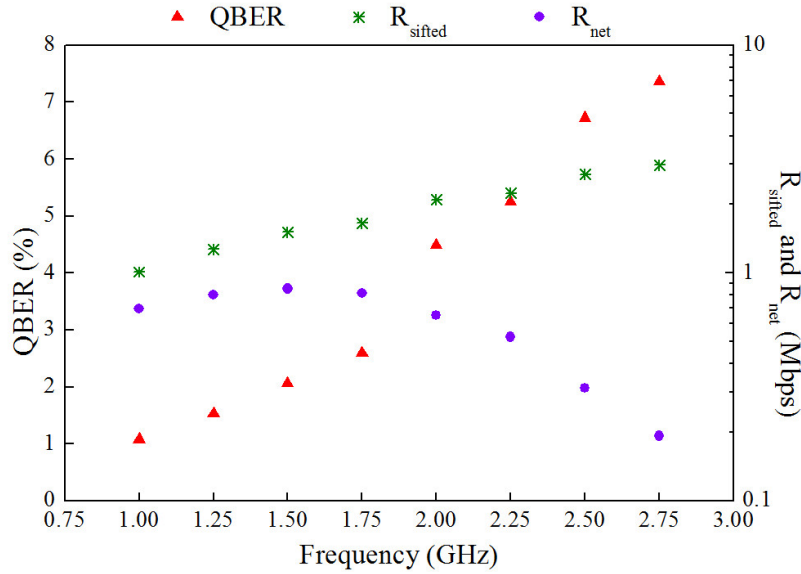
The implemented free-space QKD system was characterised for two links of 30 and 300 meters. The measurements were performed to establish the system's optimum clock frequency, the system's optimum mean photon number per pulse, the influence of solar radiation, and the system's stability and robustness

to misalignment. The different experiments and the results obtained will be described in detail in the following subsections.

### 6.3.1 Optimum clock frequency

For the characterisation of the system's optimum clock frequency, measurements of  $R_{sifted}$  and the QBER at different clock frequencies were performed. From these measurements  $R_{net}$  was estimated following Eq. 6.4. Since the solar background radiation varies depending on the time of the day, weather conditions etc., i.e., it is not a fixed contribution and cannot be easily subtracted, the measurements were taken at night to eliminate this influence on the QBER.

Figure 6.3 shows the QBER,  $R_{sifted}$  and  $R_{net}$  for the 30 m link.  $R_{sifted}$  is directly proportional to the clock frequency as more pulses containing photons are emitted per second.



**Figure 6.3** – Quantum bit error rate (left-hand axis), sifted bit rate,  $R_{sifted}$ , and secure key rate,  $R_{net}$ , (right-hand axis) against clock frequency for a 30 meter optical link.

However, the QBER increases with clock frequency due to intersymbol interference, which is caused by the timing jitter of the system, resulting in

photon events being detected in contiguous bit periods. The maximum contribution to this source of error is caused by the detectors —typically the timing jitter of the detectors ranges between 600 and 900 ps [Gordon et al., 2005], whereas the timing jitter of the emitter and the timestamp card combined was less than 200 ps.

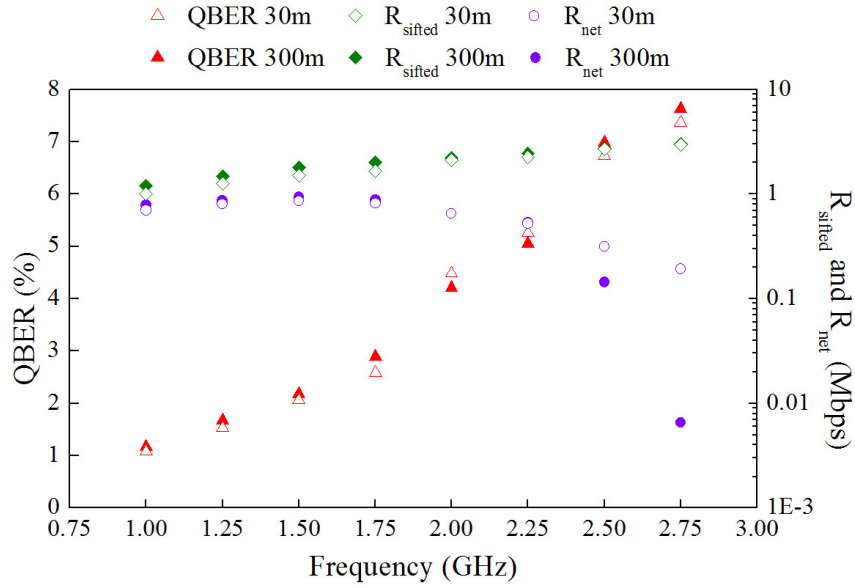
The general behaviour of  $R_{net}$  is affected by both the QBER and  $R_{sifted}$ . Obviously the larger the bit rate received by Bob the more secure bits that will be generated. However this is not true above a certain value of the QBER. Looking at Figure 6.3, for low values of the QBER (less than 3%)  $R_{net}$  increases with the clock frequency, since the effect of a higher  $R_{sifted}$  is dominant. However, for higher error rates  $R_{net}$  starts to decrease as more bits need to be discarded than those gained from  $R_{sifted}$ . From Figure 6.3 it can also be seen that the optimum clock frequency that provides the highest  $R_{net}$  is 1.5 GHz, with a QBER of 2.06% and an  $R_{net}$  of 0.85 Mbps.

The system's characterisation against repetition rate was also performed for a distance of 300 m, and the sifted bit rate and the QBER were again measured at different clock frequencies. The secret or net bit rate was estimated following Eq. 6.4 from the measured values of  $R_{sifted}$  and QBER. The experiment was anew carried out at night to operate in absence of solar background radiation, so that background rate was negligible and above all, constant. The experiment yielded very similar results to those achieved in the 30 m experiment, as shown in Figure 6.4. It must be stressed that the loss of the system had a deviation of approximately  $\pm 0.5$  dB, what was thought to be due to factors such as slight errors in the alignment, the temperature dependence of the narrowband filter's transmission in Bob, the degree of beam wander—which also depends on the temperature and weather conditions—, etc. This would explain the slightly higher sifted bit rate at 300 m than that at 30 m in some cases, and hence a certain improvement in the maximum net bit rate at 1.5 GHz (from 0.85 Mbps at 30 m to 0.93 Mbps at 300 m). However comparable results were observed in general for both 30 m and 300 m links regarding the QBER,  $R_{sifted}$ , and  $R_{net}$ .

For high values of the QBER ( $>5\%$ ) the difference in  $I_{AE(USD)}$  between both links (Eve eavesdrops less photons for shorter distances since the loss of the channel that she can compensate is lower) has a higher impact on  $R_{net}$ ,



and the fraction of bits from the sifted key that need to be discarded in the privacy amplification process is much higher for the 300 m link than for the 30 m link. Hence the higher  $R_{net}$  values for the 30 m link at clock frequencies  $\geq 2.5$  GHz.



**Figure 6.4** – Comparison between both optical links in terms of quantum bit error rate (left-hand axis), sifted bit rate,  $R_{sifted}$ , and secure key rate,  $R_{net}$ , (right-hand axis) as a function of the clock frequency.

Since no relevant parameters were changed from the 30 m link to the longer link, except for a higher attenuation in the transmission channel, at 300 m the optimum clock frequency which provided the highest  $R_{net}$  was also 1.5 GHz. All the experiments discussed in the following subsections were clocked at this frequency (except for the characterisation of the influence of solar radiation at 30 m, which will be later explained).

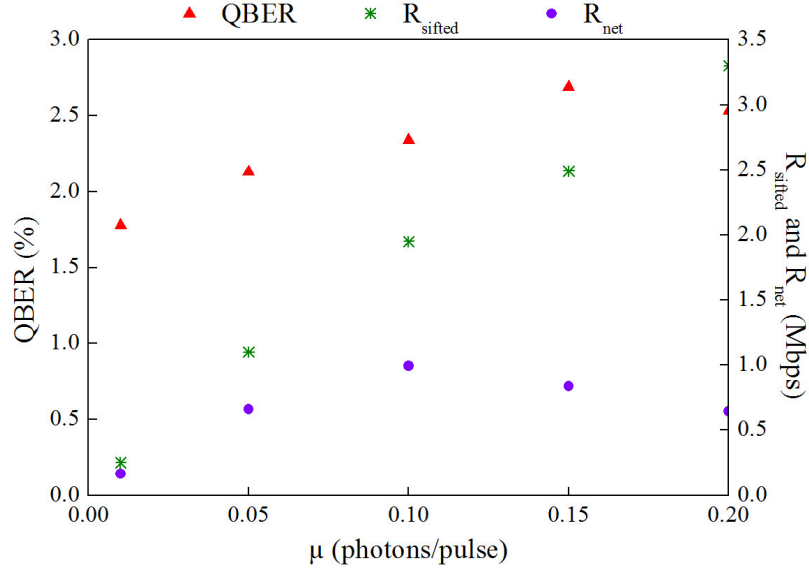
From Figures 6.3 and 6.4 it can also be inferred that if the computed error rate is above a certain value, which for our system is  $\sim 8\%$ , no secure key can be extracted from the sifted key after the error correction and privacy amplification processes ( $R_{net} \leq 0$ ).



### 6.3.2 Optimum mean photon number per pulse

The choice of  $\mu$  is the subject of considerable work [Lütkenhaus, 2000], and is determined by the characteristics of the system, the QKD protocol implemented, etc. Therefore, an experiment was performed to find out the value of  $\mu$  that provided the highest  $R_{net}$ . Concretely, measurements were made to establish the QBER and  $R_{net}$  for different values of  $\mu$  at a fixed clock frequency of 1.5 GHz.

Decreasing  $\mu$  decreases the probability (given by Poisson distribution) of finding more than one photon in a nonempty pulse, and therefore, the information gained by Eve in the case of a PNS attack taking place ( $I_{AE(PNS)}$ ). This means that less photons need to be discarded in the privacy amplification process, what can be clearly seen in Figure 6.5 for  $\mu \sim 0.01$  photons per pulse (the lowest characterised value of  $\mu$ ), where  $R_{sifted}$  and  $R_{net}$  are almost identical since the multiphoton fraction is so small that Eve can gain almost no information from a PNS attack.



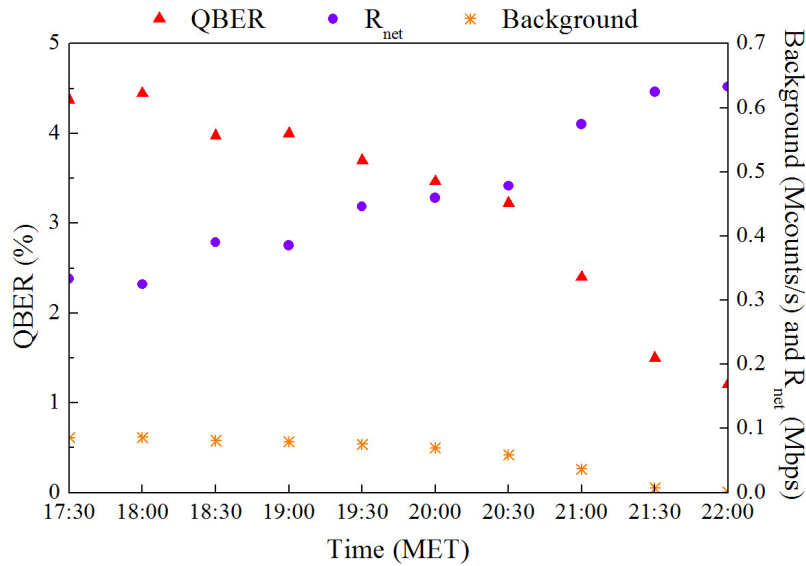
**Figure 6.5** – Quantum bit error rate (left-hand axis), sifted bit rate  $R_{sifted}$  and secure key rate  $R_{net}$  (right-hand axis) against the mean photon number per pulse  $\mu$  for a 300 meter optical link.

However, decreasing  $\mu$  also decreases the number of photons per pulse that Alice emits, and therefore the detected photon rate at Bob, i.e.,  $R_{sifted}$ . Hence

there is a trade-off between security and sifted bit rate. The optimum compromise is achieved for  $\mu \sim 0.1$  since it enables the highest value of secret key rate  $R_{net}$ . It must be said that higher values of  $\mu$ , without jeopardising the security and therefore enabling higher secure key rates, are possible if a decoy-state protocol were implemented, as reported in [Lucamarini et al., 2009]. Figure 6.5 shows the QBER,  $R_{sifted}$  and  $R_{net}$  for the 300 m link. The results for the 30 m link are not shown since no significant differences between both links were found.

### 6.3.3 Influence of background radiation

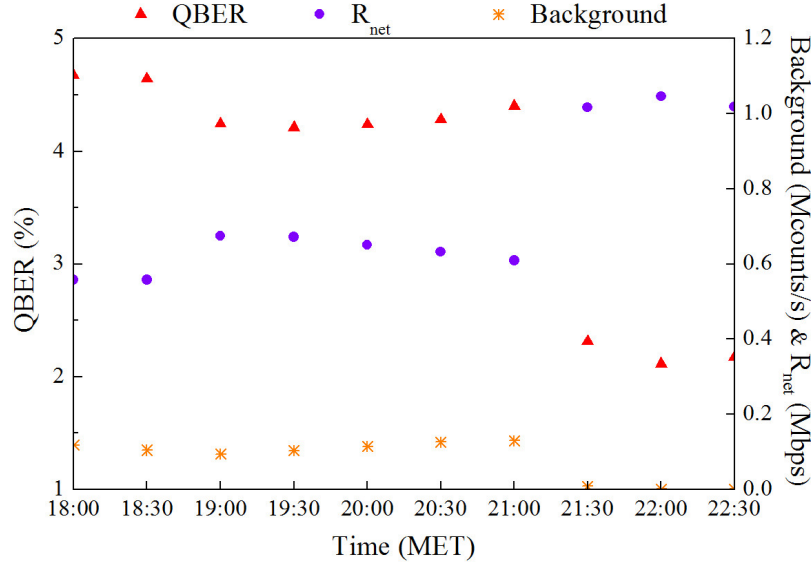
The influence of the solar background radiation on the performance of the system was characterised by measuring the QBER,  $R_{sifted}$  and the background rate at different times of the day.  $R_{net}$  was calculated following Eq. 6.4 from the measured values of  $R_{sifted}$  and QBER. Figures 6.6 and 6.7 show the QBER,  $R_{net}$  and the background rate for the 30 m and the 300 m links respectively.



**Figure 6.6** – Quantum bit error rate (left-hand axis), background rate and secure key rate  $R_{net}$  (right-hand axis) measured the 22<sup>nd</sup> of May 2012 for a 30 meter optical link at a clock frequency of 1 GHz.

The experiment was performed firstly for the 30 m link under bright sunny conditions on May 22<sup>nd</sup> 2012, when sunset started at 21:29. The clock frequency was set to 1 GHz, since this experiment was performed prior to the

experiment that established the optimum clock frequency of the system (1.5 GHz). The same experiment for the 300 m link was carried out on July 31<sup>st</sup> 2012 (sunset starting at 21:32), but this time at 1.5 GHz.



**Figure 6.7** – Quantum bit error rate (left-hand axis), background rate and secure key rate  $R_{net}$  (right-hand axis) measured the 31<sup>st</sup> of July 2012 for a 300 meter optical link at the optimum clock frequency (1.5 GHz).

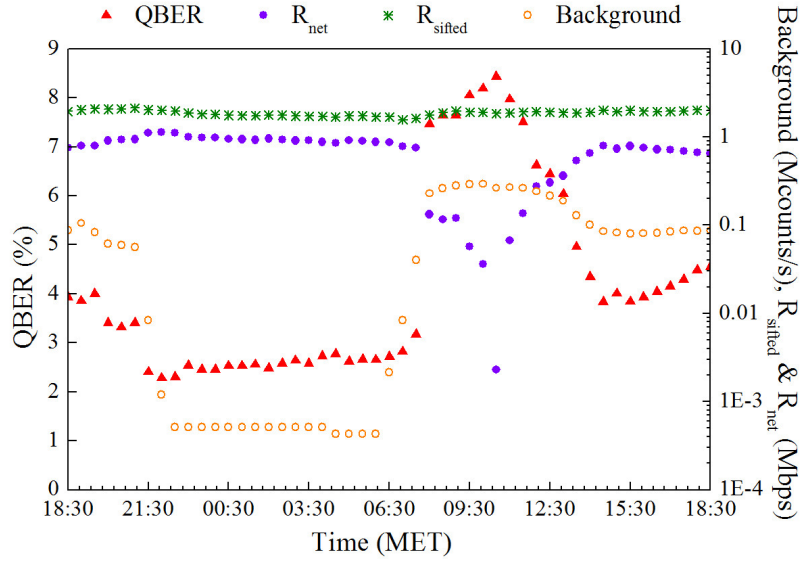
There is a different trend in both the background rate and QBER for the 300 m link compared to the 30 m, consisting mainly in a sharper decrease in both variables with a slight increase just before falling. This was due to the sun rays hitting directly the emitter from 19:00 to 21:00, which coupled directly into the emitter causing the background rate and QBER to increase. The background rate and QBER then decrease significantly coinciding with the sunset, and the secret key rate  $R_{net}$  then reaches its maximum, 0.63 Mbps for the 30 m link and 1.04 Mbps for the 300 m link. Before sunset, a mean secure key rate of 0.4 Mbps and 0.6 Mbps respectively, in full bright solar conditions was demonstrated.

### 6.3.4 Stability of the system

The stability of the link was tested to characterise the maximum time the system stayed aligned and operating without human intervention. For that purpose the alignment of the link was optimised before the experiment started

and not touched after that for a period of 24 hours. The QBER and  $R_{sifted}$  were then measured every 30 minutes during this period. It should be stressed that daylight measurements were taken under bright sunny conditions and hence a high background radiation was present (June 14<sup>th</sup> and July 24<sup>th</sup> for the 30 m and the 300 m links respectively).

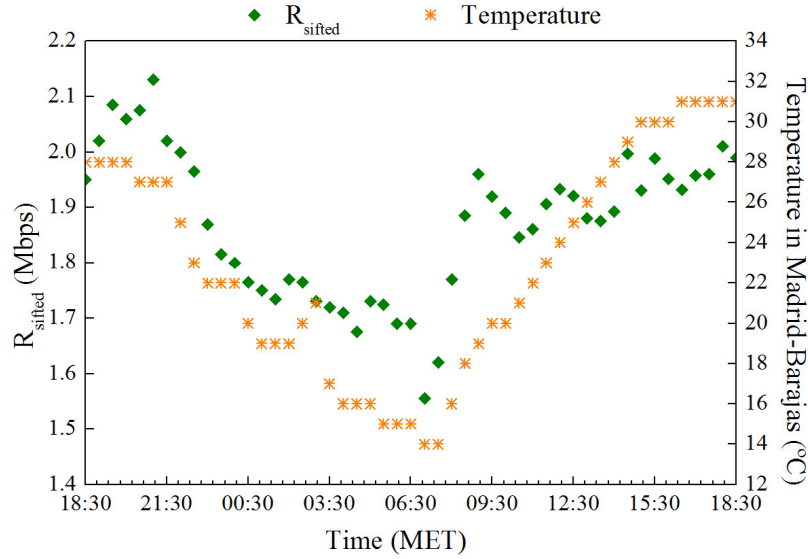
Figure 6.8 represents the QBER,  $R_{net}$ ,  $R_{sifted}$  and background rate for the 30 m optical link. It shows that once aligned, the system remained operational for 24 hours without any adjustment, with a QBER between 2.3% and 8.4%. The maximum measured secure key rate was 1.13 Mbps, the minimum was 2.3 kbps and the average value throughout the whole day 0.7 Mbps. A period of approximately 5 hours can be identified, in which the secret key rate is below its average value. This drop in  $R_{net}$  was due to a straight incidence of the sun rays on the receiver telescope from 2 hours after the sunrise until close to zenith time, which caused a higher background rate and hence higher QBER.



**Figure 6.8** – Quantum bit error rate (left-hand axis), sifted bit rate  $R_{sifted}$ , secure key rate  $R_{net}$ , and background count rate (right-hand axis) during a 24-hours experiment for a 30 meter optical link. The experiment was performed under bright summer conditions from the 13<sup>th</sup> to the 14<sup>th</sup> of June 2012.

A more detailed analysis of the measurements shows that the sifted bit rate varied with temperature. Figure 6.9 shows how the rate of detected photons in Bob, i.e.,  $R_{sifted}$ , decreased coinciding with a drop in temperature along the

24-hours experiment carried out on June 14<sup>th</sup>. This could be explained by the temperature dependence of the narrowband filter's transmission in the receiver, and by the thermal expansion of the system's components and the buildings, which could cause a temporal misalignment between both telescopes.

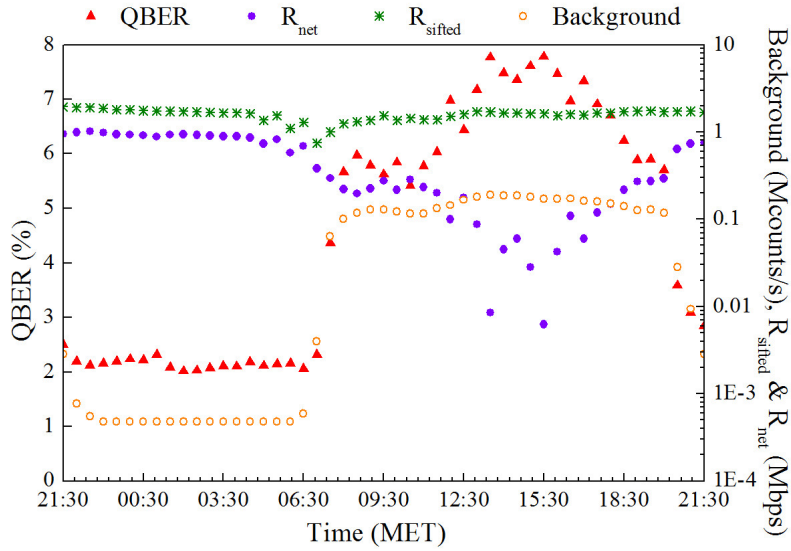


**Figure 6.9** – Sifted bit rate (left-hand axis) and temperature data from Madrid-Barajas meteorological station (right-hand axis) along a 24-hours experiment run from the 13<sup>th</sup> to the 14<sup>th</sup> of June 2012.

The stability of the system was also tested for the 300 m link. The QBER,  $R_{sifted}$  and background rate were again acquired every 30 minutes for an uninterrupted period of 24 hours (the 24<sup>th</sup> of July). These magnitudes and the calculated  $R_{net}$  are represented in Figure 6.10. The QBER ranged between a minimum of 2% in nighttime conditions and a maximum of 7.8% during the day. The period with a high QBER (between 7% and 8%) for the 300 m link was longer compared to such period for the shorter link. This was due to the different orientations of the facades of the receiver locations. The receiver's window for the 300 m link was oriented to the south, in contrast to the 30 m link where the receiver's window had an east orientation. This meant that for the shorter link the sun did not directly hit the receiver after midday, whereas for the 300 m link the receiver was exposed to the sun rays during almost the whole day.

The maximum measured secure key rate at 300 m was 1 Mbps, whereas the minimum was 4.5 kbps, being the average value throughout the whole day 0.5 Mbps. The system's performance proved very stable, with the capability of running continuously for 24 hours without human interaction since after this period  $R_{sifted}$  and  $R_{net}$  took values of 87% and 80%, respectively, of their initial values.

The maximum secret key rate  $R_{net}$  (1 Mbps) is more than one order of magnitude higher than those of other systems operating at the same range of distances [Hughes et al., 2002b], [Weier et al., 2006], and the corresponding  $R_{sifted}$  (1.8 Mbps) more than 4 times the highest value reported to date for field experiments [Bienfang et al., 2004].



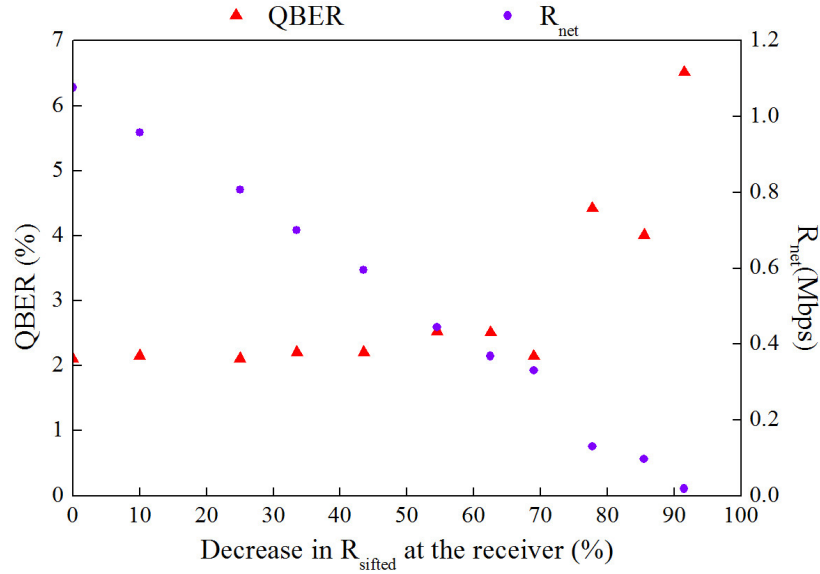
**Figure 6.10** – Quantum bit error rate (left-hand axis), sifted bit rate  $R_{sifted}$ , secure key rate  $R_{net}$ , and background count rate (right-hand axis) during a 24-hours experiment for a 300 meter optical link. The experiment was performed under bright summer conditions from the 23<sup>rd</sup> to the 24<sup>th</sup> of July 2012.

### 6.3.5 System robustness to misalignment

The robustness of the system to vibrations and other sources of misalignment was tested by purposely misaligning the emitter from the receiver from an optimised alignment of the 300 m link with an established transmission at the optimum frequency (1.5 GHz). The misalignment was calculated from the

decrease in the sifted bit rate at the receiver as a percentage from its highest value, which corresponds to the system being perfectly aligned. Figure 6.11 shows that it was only after 90% of misalignment (this means that Bob has lost 90% of the initial  $R_{sifted}$  when the system was perfectly aligned) that the QBER reached values higher than 6%. Still secret key rates of 18 kbps with this degree of misalignment were measured.

The decrease in the sifted bit rate of 13.4% after the 24-hours period discussed in the previous section was likely caused by relative pointing deviations, mainly due to building sway and thermal fluctuations. Figure 6.11 shows that it is only after a misalignment of at least 60% that the QBER increases slightly (0.3%) and after 70% that this increase in the error is more noticeable. This tendency shows that the system could potentially be aligned for 4 or 5 days without external intervention at 300 meters.



**Figure 6.11** – Quantum bit error rate (left-hand axis) and secure key rate  $R_{net}$  (right-hand axis) against an intentionally-caused misalignment at the emitter.

## 6.4 Characterisation of the contributions to the QBER

The calculation of the QBER has been described in section 6.2.1 and, as mentioned in section 2.4.1, it can also be expressed as the addition of three

contributions:

$$QBER = QBER_{PL} + QBER_{ISI} + QBER_{BCK} , \quad (6.5)$$

where  $QBER_{PL}$  is a base error rate resulting from imperfections in the optics of the system, which causes *polarisation leakage*, i.e., photons that are detected in the wrong channel due to the ellipticity of the non-orthogonal polarisation states —as opposed to perfect linearly polarised states. This contribution to the QBER is originated mainly by the different effects that degrade the polarisation of the quantum states, such as the intrinsic birefringence of some optical components or by the reflection in Alice’s beamsplitter cube and mirrors, as discussed in section 3.4.  $QBER_{ISI}$  is the error rate due to inter-symbol interference, which is caused by the timing jitter of the single-photon detectors in the most part, as discussed in section 6.3.1. Finally,  $QBER_{BCK}$  is the error rate contribution due to background radiation and dark counts of the detectors.

$QBER_{PL}$  keeps invariable once the system has been implemented, since this term depends on the optical components used.  $QBER_{ISI}$  varies with the clock frequency, and it arises at clock rates in excess of  $\sim 1$  GHz for the timing jitter of our system.  $QBER_{BCK}$  depends on the background conditions of each key exchange, which in turn depend on the time of the day, the location and orientation of the optical link, the weather conditions, etc., as discussed in section 6.3.3.

To estimate  $QBER_{PL}$  the polarisation extinction ratio of both quantum states was measured at the end of both channels in Bob (see section 5.5). The PER values were then used to calculate the ratio of the percentage of photons with the ‘unwanted’ polarisation to the percentage of photons with the right polarisation that are detected in each channel. Also the background count rate was measured for each key exchange in order to determine  $QBER_{BCK}$ , which was calculated as the ratio of background events per second to twice the total number of detected events per second. The factor 2 in the denominator is due to the fact that only half of the background counts really contribute to the error, as the other half fall into the right bit windows simply by chance. Finally,  $QBER_{ISI}$  was measured at different clock frequencies by directly connecting the source of single photons, i.e., the attenuated VCSELs, to the SPADs,



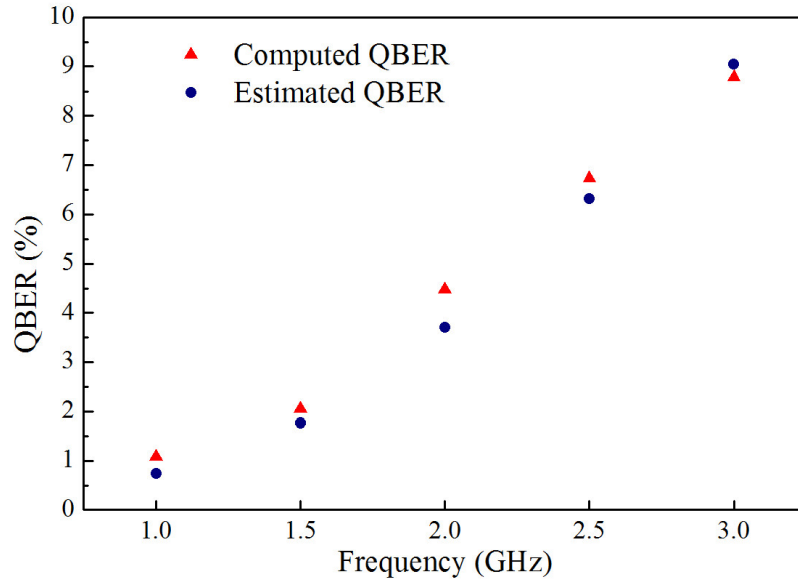
thus eliminating the remaining contributions:  $QBER_{PL}$ , since no B92 scheme was implemented, i.e., photon detection did not depend on the polarisation of the photons, indeed the photons were not polarised as no optical elements were placed in the setup; and  $QBER_{BCK}$ , since no background photons could be leaked into the detectors as it was all connected by optical fibre and the experiment was run in darkness. The obtained values of  $QBER_{ISI}$  can be seen on Table 6.1, which clearly shows that the error rate increases with the clock frequency since more photons are detected in adjacent time windows.

**Table 6.1** – Quantum bit error rate due to intersymbol interference at different clock frequencies.

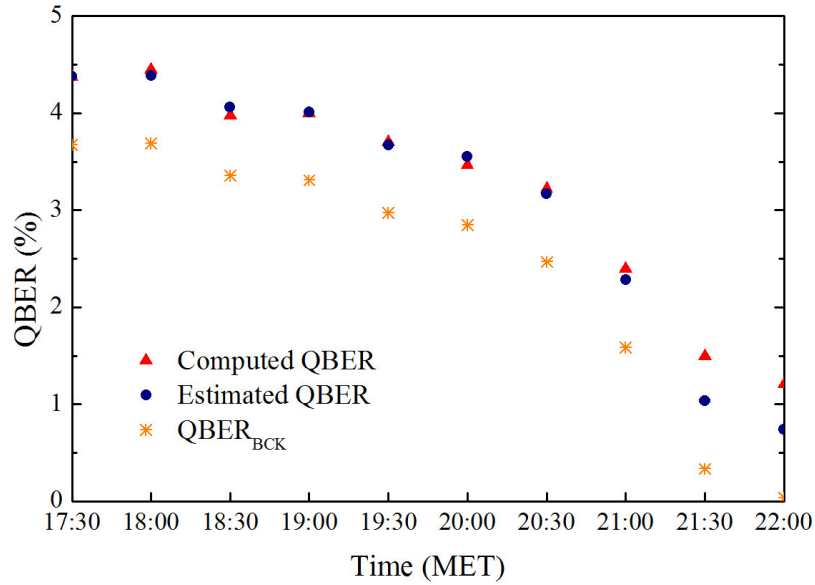
Frequency (GHz)	1.0	1.5	2.0	2.5	3.0
$QBER_{ISI}$ (%)	0.47	1.51	3.46	6.08	8.80

The ‘standard’ QBER computed from a key exchange was compared to that calculated measuring each contribution separately as discussed above. In the experiment carried out to establish the optimum clock frequency for the operation of the system, the error component due to background radiation was almost negligible ( $< 0.02\%$ ) since the experiment was performed at night, when the background rate was around 550 counts/s in total ( $\sim 225$  counts/s per detector). The error due to polarisation leakage was calculated to be  $0.23\%$ . Finally, the values of the error caused by intersymbol interference were those shown in Table 6.1, being the most significant contribution to the error. The addition of these three components is represented in Figure 6.12 (which we shall call *estimated* QBER to distinguish it from the standard *computed* QBER), and it can be seen that both values are very similar.

Figure 6.13 shows a comparison between the estimated and computed QBER values taken in the study of the influence of the solar background radiation on the system at a distance of 30 m. The error component due to background,  $QBER_{BCK}$ , is the most significant error source until sunset, and it is also represented in the graph. The error due to polarisation leakage was  $0.23\%$ , and the error caused by intersymbol interference was that corresponding to a clock frequency of 1 GHz ( $0.47\%$  from Table 6.1). The addition of these three sources of error yields the expected values for the QBER, which agree with the actual computed QBER values from the test events disclosed by Alice.



**Figure 6.12** – Comparison of computed QBER with estimated QBER at different clock frequencies for the 30 meter optical link.



**Figure 6.13** – Comparison of computed QBER with estimated QBER and the QBER component due to background radiation measured the 22<sup>nd</sup> of May 2012 for a 30 meter optical link operating at a clock frequency of 1 GHz.

This analysis of the different contributions to the QBER reveals that the main component of the error rate in daytime is caused by the background

radiation, while at night the main contribution is due to intersymbol interference.

## 6.5 Maximum achievable distance and turbulence

Although the QKD system presented in this thesis has only been experimentally tested for distances up to 300 m, it has been designed to withstand longer distances. To simulate the maximum transmission distance the system could operate at, it is essential to take into account the effect of turbulence.

The effects of atmospheric turbulence that most influence a QKD link are *beam spreading* and *beam wander*. As discussed in section 4.1.3, the former is caused by turbulent eddies that are small compared to the beam diameter, and its overall effect is an increase in the ‘natural’ beam divergence of the beam. Beam wander, on the other hand, is due to turbulent eddies that are large compared to the beam diameter, and it causes random deflections of the beam. Both effects can be modelled by a *long term beam radius* ( $w_{LT}$ ) at the receiver [Andrews et al., 2005]. This radius depends on the turbulent regime, which is characterised by the *refractive index structure constant*  $C_n^2$ . Different regimes of turbulence have been considered and the corresponding beam radii  $w_{LT}$  have been calculated. Then the geometrical loss for each Gaussian beam of radius  $w_{LT}$  at the receiver has also been calculated, and with this loss the maximum transmission distance of the system has been approximated.

In the absence of turbulence, the maximum transmission distance the system could operate at, can be estimated by using the sifted bit rate measured for the characterisation of the system robustness to misalignment discussed in section 6.3.5. A reduction of 90% in  $R_{sifted}$ , which would leave a secret key rate of only 18 kbps, corresponds to a loss of 10.71 dB. Considering the attenuation of the atmospheric channel with the same urban aerosol conditions of previous experiments (2.04 dB/km), and no turbulence, such loss allows links of up to 5.2 km. If the turbulence is now taken into account, this distance is reduced depending on the strength of the turbulence to the values presented on Table 6.2. For a regime of weak turbulence ( $C_n^2 \approx 10^{-16}$ ) or a regime of intermediate turbulence ( $C_n^2 \approx 10^{-15}$ ), our calculations show that the system could potentially operate up to a distance of 4.4 km, with a secret key rate at night

of 18 kbps. For a stronger turbulence regime ( $C_n^2 \approx 10^{-14}$ ) the distance drops to 3.4 km. Refractive index structure constants of  $C_n^2 \approx 10^{-13}$  are considered a very extreme and unlikely regime, and in that case the link could only work up to 1 km.

**Table 6.2** – Maximum transmission distance the QKD system can withstand considering several regimes of turbulence, which lead to different geometrical losses of the beam at the receiver.

	Very weak turbulence $C_n^2 = 10^{-17}$	Weak turbulence $C_n^2 = 10^{-16}$	Intermediate turbulence $C_n^2 = 10^{-15}$	Strong turbulence $C_n^2 = 10^{-14}$	Very strong turbulence $C_n^2 = 10^{-13}$
Loss caused by turbulence (dB)	1.21	1.22	1.51	3.67	8.49
Maximum achievable distance (km)	4.58	4.57	4.43	3.39	1.07

## 6.6 Conclusions

In this chapter the characterisation of the free-space QKD system for two optical links of different distance (30 and 300 meters) in downtown Madrid has been described. The alignment techniques, coarse and fine, implemented to optimise the signal acquisition in Bob have been also presented. For the coarse alignment a visible laser at a wavelength of 650 nm was sent in parallel with the beams at  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm, and Alice's DC motors were tweaked until the visible laser was spotted in the receiver. Then the fine pointing was performed by alternatively slightly modifying Alice's and Bob's positions by using their motors, as well as by adjusting the  $xyz$  mounts of each channel in Bob, until the detected signals at  $\lambda \sim 850$  nm and  $\lambda \sim 1550$  nm agreed with the expected loss for each wavelength.

Later on the steps of the key exchange protocol have been commented. The calculation of the QBER in a MATLAB routine as the ratio of wrong detected events to the total number of events has been explained. Subsequently the estimation of the final secret key rate from the QBER and the sifted bit rate, considering that the transmission has been eavesdropped by implementing both a PNS and a USD attack has been discussed.

In addition, the experiments performed to characterise the QKD system have been described for the two mentioned optical links. First, the results obtained from the measurements carried out to establish the optimum clock frequency have been presented. The experiments yielded a system's optimum operation clock rate of 1.5 GHz. Both optical links exhibited similar behaviour in terms of the QBER, sifted bit rate and secret key rate. The maximum frequency the system could operate at was 2.75 GHz with a QBER of almost 8%, which was in turn established as the maximum value of QBER supported by the system presented in this thesis, since for higher error rates no secure key can be extracted from the sifted key after the error correction and privacy amplification processes.

The optimum mean photon number for the system was also characterised. The best  $R_{net}$  was obtained for  $\mu \sim 0.1$  photons per pulse, achieving an optimum compromise between security and sifted bit rate.

The operation of the system in daytime under bright sunny conditions has been also demonstrated. Spatial and spectral filtering of the background radiation, together with light-tight shielding of emitter and receiver, enabled full-bright daylight operation with average secret key rates reaching 0.7 Mbps for a link of 30 m and 0.5 Mbps at 300 m. At nighttime conditions secure key rates of up to 1 Mbps were achieved. This secret key rate is one order of magnitude higher than those previously reported.

The stability of the system has been tested during a 24-hours experiment without human interaction. The system proved very stable since after this period the sifted and secret key rates obtained were 87% and 80% respectively, of the initial values for the 300 m link. In addition, it has been also confirmed that the orientation and location of the optical link has an influence on the amount of background radiation that is coupled into the system. Straight incidence of solar rays increases significantly the background rate and hence the QBER.

The system's robustness to misalignment has been also characterised, and it has been shown that it was only after a reduction of 90% in the sifted bit rate at Bob that the QBER reached values higher than 6%. Additionally, the maximum distance the system could withstand has been estimated considering different turbulence regimes. The simulations revealed that for a regime of

intermediate turbulence ( $C_n^2 \approx 10^{-15}$ ) the system could potentially operate up to a distance of 4.4 km.

Finally, the different contributions to the QBER have been analysed. It has been showed that the QBER can be separated into three components:  $QBER_{PL}$  due to the ellipticity of the non-orthogonal polarisation states, which causes polarisation leakage;  $QBER_{ISI}$  caused by the timing jitter of the system, which generates intersymbol interference; and  $QBER_{BCK}$  due to the background radiation and dark counts of the detectors. These three components of the QBER have been characterised and their addition has been compared to the computed QBER from the test events disclosed by Alice for two different key exchanges. The comparison shows an agreement between the QBER calculated adding the mentioned contributions and the QBER computed from the test events.

# Chapter 7

## Conclusions and future work

This chapter is intended to summarise the results and conclusions obtained in the course of the implementation and characterisation of the QKD system presented in this thesis. The contributions of this work to the field of quantum cryptography are also remarked. Finally, several indications about possible upgrades and modifications to the presented QKD system that could increase its secret key rate and transmission distance are proposed.

### 7.1 Conclusions

In this thesis a detailed description of a free-space quantum key distribution system that implements the B92 protocol at high key transmission rates in an urban scenario has been provided. The most relevant conclusions drawn from the study of the subject and the design and characterisation of the system are summarised in the following.

1. Theoretically, QKD in tandem with the one-time pad offers the highest level of security out of any encryption technique developed so far and

a secure prospect in a future with quantum computers taking part of every day's life. However, it still faces some challenges to become truly competitive, such as better robustness against side channel attacks and the achievement of higher distances and higher secret key rates.

2. When dealing with experimental implementations of QKD systems, eavesdroppers can obtain information from the 'fingerprints' left by the physical devices used in them. A QKD system must carefully be designed to take into account all possible experimental loopholes and to bound the leakage of information they may cause in order to establish the appropriate security proofs. However, the debate about the right strategies to follow in order to achieve secure QKD in the presence of loopholes is intense and very open [Yuan et al., 2011b]. No satisfactory solution has yet been devised, which emphasises that a more general security proof incorporating imperfect devices is needed [Lydersen, 2011]. An approach to eliminate all loopholes has been proposed by Acín *et al.* through *device independent quantum cryptography* [Acín et al., 2007], although the real implementation of these new protocols is technologically challenging. After almost three decades from its birth quantum cryptography has reached its maturity and faces probably its most difficult challenge: unconditional security in an 'imperfect' world.
  
3. To achieve high transmission rates the transmitter implemented in the discussed QKD system uses two high-bandwidth VCSELs driven by a fast GHz pulse pattern generator. The single-photon emission regime is achieved by attenuating the laser diodes to a mean photon number of approximately 0.1 photons per pulse. The VCSELs were optimised in terms of their driving conditions (bias and modulation currents) to minimise their contribution to the error rate caused by intersymbol interference. The optimal bias current was 2 mA and the optimal modulation current  $\sim 6$  mA, with a contribution to the QBER of less than 0.5% at a clock frequency of 1 GHz. The study of the spectra of the lasers revealed that they hardly shifted with modulation current, clock frequency and time. The spectral shift with bias current was of  $\sim 0.15$  nm/mA for high values of the bias current, and of around half for low bias currents.



4. The receiver of the QKD system analyses the polarisation of the arriving photons according to the B92 protocol. Two SPADs have been chosen as the detectors of the system due to their high efficiency, low noise, practicality and commercial availability. The characterisation of four Si-SPADs in terms of their detection efficiency, dark-count rate and contribution to the QBER was carried out. The two SPADs with the best performance showed detection efficiencies of 29% and 35%, and dark-count rates of 170 and 250 counts/s, respectively. The timestamp card used to record the times of arrival of the detected photons was a GT658PCI Time Interval Analyser from GuideTech. The LabVIEW user interface supplied with the card was modified to monitor the count rate at each input channel and to provide the lists of arrival times for each polarisation state.
5. Two telescopes were used at each end of the QKD system to enhance the collection of photons emitted by Alice. In Bob, in addition to the Schmidt-Cassegrain telescope, two imaging lenses with 30 mm focal length have been mounted to improve the beam coupling into the fibres.
6. For the alignment between both stations, Alice was mounted on a high-precision gimbal system with two rotation motors, which provided the azimuth and elevation movements needed for the correct aiming of Alice towards Bob. The receiver optical module was directly attached to the Schmidt-Cassegrain telescope, and its motors allowed the alignment with the transmitter station. Also a visible laser at a wavelength of 650 nm was sent in parallel with the data and synchronisation beams to facilitate the coarse alignment.
7. The non-orthogonal polarisation quantum states encoding the binary data are transmitted through free space from Alice to Bob. The atmosphere is an excellent transmission channel due to its non-birefringence, which preserves the polarisation states of the photons. Moreover, in the proximity to  $\lambda \sim 850$  nm there is a low absorption window, where efficient single-photon detectors are available. However, factors such as atmospheric attenuation, weather conditions and turbulence limit the maximum achievable transmission distance. The experiments presented in this thesis were carried out for two optical links in downtown Madrid.

The attenuation of the links calculated with MODTRAN, considering urban extinction with a visibility of 5 km, was  $\sim 2$  dB/km for the beam at  $\lambda \sim 850$  nm. In addition, calculations were done to estimate the geometrical loss of the beam at the receiver under several turbulence regimes. The simulations revealed that for a regime of intermediate turbulence ( $C_n^2 \approx 10^{-15}$ ) the system could potentially operate up to a distance of 4.4 km.

8. Free-space QKD systems are also affected by the solar background radiation and other sources of ambient light, which may couple into the system and increase the error rate. Spectral and spatial filtering have been implemented, as well as the isolation of Alice and Bob by means of light blackout fabric and a long antireflective tube around the main lens of Alice telescope. The 1 nm FWHM interference filter reduced the background by 30 dB, and the spatial filtering carried out by optical fibres with a core diameter of  $62.5 \mu\text{m}$  gave the receiver a restricted field of view. These filtering and isolation measures allowed daylight operation at high transmission rates.
9. The polarisation extinction ratio of both non-orthogonal quantum states at  $\lambda \sim 850$  nm was characterised throughout the whole QKD system. In general, the absorption inherent to the materials of certain optical components degraded the linearity of the polarisation states, being dramatically more noticeable for the diagonal state. A quarter-wave plate in Alice and two quarter-wave plates in conjunction with a half-wave plate in Bob were used to counteract such effect, obtaining polarisation extinction ratios that contributed to the total QBER with less than 0.25% due to polarisation leakage.
10. An optical synchronisation between Alice and Bob at a different wavelength from that used for the data was implemented. It consisted in Alice sending a periodic bright pulse at a wavelength of 1550 nm and at a repetition rate of 10 MHz. The electrical synchronisation signal was obtained from the trigger output of the generator in the transmitter, which modulated a  $\lambda \sim 1550$  nm VCSEL. In Bob an InGaAs photodetector was used for the detection of the synchronisation signal, and a trans-impedance

amplifier enhanced its voltage level to satisfy the voltage requirement at the external-clock input of the timestamp card.

11. The transmission efficiency of the channel (0.87 at 300 m), the overall efficiency of the receiver optics (0.14), the detection efficiency of the SPADs (0.32), and the efficiency of the B92 protocol (0.25), yielded a total efficiency of 0.01 for an optical link of 300 m.
12. The free-space QKD system was characterised for two optical links of different distance, 30 m and 300 m, in an urban area. The secret key rate was calculated from the measurements of the QBER and sifted bit rate assuming a worst case scenario with two simultaneous eavesdropping attacks taking place: the USD and the PNS attack. The following results were obtained from the characterisation of the system:
  - The system's optimum operation clock frequency, i.e., that one providing the highest secret key rate, is 1.5 GHz. The maximum frequency the system can operate at is 2.75 GHz with a QBER under 8% in nighttime conditions.
  - The optimum mean photon number is  $\mu \sim 0.1$  photons per pulse, for which an optimum compromise between security and sifted bit rate is achieved.
  - The operation of the system in daytime under full bright sunny conditions has been demonstrated, with average secret key rates reaching 0.7 Mbps for a link of 30 m, and 0.5 Mbps for the 300 m link.
  - At nighttime conditions secure key rates of up to 1 Mbps at a distance of 300 m were achieved. This secret key rate is one order of magnitude higher than those previously achieved by similar systems in comparable conditions.
  - The system proved very stable since for an experiment run over a 300 m optical link, after a period of 24 hours and no human intervention, the sifted and secret key rates obtained were 87% and 80% of their initial values (at the beginning of the experiment) respectively.

- The system's robustness to misalignment showed that it was only after a reduction of 90% in the sifted bit rate at Bob that the QBER reached values higher than 6%. This tendency indicated that the system could potentially remain aligned at 300 meters for 4 or 5 days without external intervention.

## 7.2 Future work

As mentioned in the first conclusion, there are some aspects like unconditional security, transmission distance or secret key rates, where a special effort should be made for experimental realisations of QKD to become truly competitive.

Regarding security, the future plan of research involves the upgrade of the QKD system presented in this thesis to implement the more secure BB84 with decoy-state protocol. This will make the system invulnerable to PNS and USD eavesdropping attacks, and will also increase the secure key rate by at least one order of magnitude. For this, some additional optics to include the additional polarisation states, two more VCSELs in Alice, two more detectors in Bob, as well as intensity modulators to generate the different intensities of the decoy states, should be employed.

To make the system more robust against possible eavesdropping attacks, it is essential to ensure that the laser sources are totally indistinguishable so that no extra information is provided to the eavesdropper. The VCSELs are power stable since the drivers of the lasers contain an automatic power control circuitry, which maintains an average optical power output over changes in temperature and laser properties. This control may slightly vary the bias current of the laser, what could shift its emission spectrum. In order to ensure a stable emission wavelength it is foreseen to control the temperature of the lasers. This would allow fine tuning the emission wavelength of the VCSELs to a precise desired wavelength, identical for both lasers. Moreover, since both VCSELs are multimode, a narrow bandpass filter would be used to ensure that only one spectral mode propagates.

In regard to secure key rates, they could be improved by reducing the QBER of the key transmissions. In daylight, the main contribution to the QBER is the background radiation. To reduce the background light collected by the system

a new configuration of Alice where the mirrors become dispensable has been designed. The implementation of the new Alice will require a rearrangement of the optics, which involves modifying the set of lenses of the telescope and the optical breadboard.

The background could also be reduced by using a narrower spatial filtering, for instance with optical fibres of a smaller diameter in Bob. However, this would also reduce the angle of acceptance of the receiver, making the system more vulnerable to turbulence effects. Therefore, a further optimisation of the system would consist in the implementation of active pointing and fast tracking techniques —currently under development— to permit continuous operation under turbulent fluctuations in the atmosphere. This would also allow increasing the distance of the optical link.

Finally, the system is currently being upgraded to perform real-time error correction and privacy amplification processes in order to distil the final secret key shared by Alice and Bob.



## References

- [Acín et al., 2004] Acín, A., Gisin, N., and Scarani, V. (2004). Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks. *Phys. Rev. A*, 69:012309. <http://arxiv.org/pdf/quant-ph/0302037v1>. 2.2.1
- [Acín et al., 2007] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., and Scarani, V. (2007). Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98:230501. <http://www.icfo.es/images/publications/J07-045.pdf>. 2, 2.4.4, 2
- [Agilent, 2007] Agilent (2007). *Agilent 81133A/81134A Pulse Generator Programming Guide. Manual Part Number 5988-7402EN*. Agilent Technologies Inc. 3.2
- [Agrawal, 2002] Agrawal, G. P. (2002). *Fiber-Optic Communications Systems, 3<sup>rd</sup> Edition*. John Wiley & Sons, Inc. ISBN: 0-471-21571-6, New York, NY (USA). 2.3.2, 3.3.1
- [Anderson et al., 1995] Anderson, G. P., Kneizys, F. X., Chetwynd, J. H., Wang, J., Hoke, M. L., Rothman, L. S., Kimball, L. M., and McClatchey, R. A. (1995). FASCODE/MODTRAN/LOWTRAN: Past/Present/Future. In *Proceedings of the 18<sup>th</sup> Annual Review Conference on Atmospheric Transmission Models*. 4.1.3
- [Anderson et al., 2000] Anderson, G. P., Berk, A., Acharya, P. K., Matthew, M. W., Bernstein, L. S., Chetwynd, Jr., J. H., Dothe, H., Adler-Golden, S. M., Ratkowski, A. J., Felde, G. W., Gardner, J. A., Hoke, M. L., Richtsmeier, S. C., Pukall, B., Mello, J. B., and Jeong, L. S. (2000).

- MODTRAN4: radiative transfer modeling for remote sensing. In *Proceedings of SPIE 4049, Algorithms for Multispectral, Hyperspectral, and Ultraspectral Imagery VI*, pages 176–183. 4.1.3
- [Andrews et al., 2005] Andrews, L. C. and Phillips, R. L. (2005). *Laser Beam Propagation through Random Media, 2<sup>nd</sup> Edition*. SPIE Press Monograph, vol. PM152. ISBN: 9780819459480, Orlando, FL (USA). 6.5
- [Aspelmeyer et al., 2003] Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W., and Zeilinger, A. (2003). Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9:1541–1551. <http://arxiv.org/pdf/quant-ph/0305105.pdf>. 2.5
- [Barrett et al., 2012] Barrett, J., Colbeck, R., and Kent, A. (2012). Memory attacks on device-independent quantum cryptography. In *Proceedings of the 2<sup>nd</sup> Annual Conference on Quantum Cryptography (QCRYPT)*. [http://2012.qcrypt.net/docs/extended-abstracts/qcrypt2012\\_submission\\_38.pdf](http://2012.qcrypt.net/docs/extended-abstracts/qcrypt2012_submission_38.pdf). 2.4.4
- [Bechmann-Pasquinucci et al., 1999] Bechmann-Pasquinucci, H. and Gisin, N. (1999). Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59:4238–4248. <http://arxiv.org/pdf/quant-ph/9807041v2.pdf>. 2.2.1
- [Bennett, 1992] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124. 2.2.1, 2.2.3, 2.2.3
- [Bennett et al., 1984] Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of International Conference on Computers Systems and Signal Processing*, volume 175, pages 175–179. Bangalore, India. <http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf>. (document), 1.1, 2.1.4, 2.2.1
- [Bennett et al., 1992a] Bennett, C., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28. <http://www.hit.bme.hu/~gyongyosi/quantum/cikkek/BBSS92.pdf>. 2.3.2



- [Bennett et al., 1992b] Bennett, C. H., Brassard, G., and Mermin, N. D. (1992). Quantum cryptography without Bell’s theorem. *Phys. Rev. Lett.*, 68:557–559. 2.2.1
- [Benton et al., 2010] Benton, D. M., Gorman, P. M., Tapster, P. R., and Taylor, D. M. (2010). A compact free space quantum key distribution system capable of daylight operation. *Optics Communications*, 283(11):2465–2471. <http://www.sciencedirect.com/science/article/pii/S0030401809010141>. 2.5, 4.1.5
- [Bienfang et al., 2004] Bienfang, J., Gross, A., Mink, A., Hershman, B., Nakassis, A., Tang, X., Lu, R., Su, D., Clark, C., Williams, C., Haggley, E., and Wen, J. (2004). Quantum key distribution with 1.25 Gbps clock synchronization. *Opt. Express*, 12(9):2011–2016. <http://arxiv.org/ftp/quant-ph/papers/0405/0405097.pdf>. 2.5, 5.3.1, 6.3.4
- [Biham et al., 1997] Biham, E. and Mor, T. (1997). Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 78:2256–2259. <http://arxiv.org/pdf/quant-ph/9605007v2>. 2.4.3
- [Bimberg et al., 2010] Bimberg, D. and Stock, E. (2010). Single photon sources based on semiconductor quantum dots. In *Proceedings of the Photonics Society Winter Topicals Meeting Series*, Majorca (Spain). 3.3
- [Bonato et al., 2009a] Bonato, C., Tomaello, A., Deppo, V., Naletto, G., and Villoresi, P. (2009). Study of the quantum channel between earth and space for satellite quantum communications. In Sithamparanathan, K. and Marchese, M., editors, *Personal Satellite Services*, volume 15 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 37–40. Springer, Berlin (Germany). <http://www.springerlink.com/index/130r386298523w91.pdf>. 2.5
- [Bonato et al., 2009b] Bonato, C., Tomaello, A., Deppo, V. D., Naletto, G., and Villoresi, P. (2009). Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017. [http://iopscience.iop.org/1367-2630/11/4/045017/pdf/1367-2630\\_11\\_4\\_045017.pdf](http://iopscience.iop.org/1367-2630/11/4/045017/pdf/1367-2630_11_4_045017.pdf). 2.5

- [Boyer et al., 2012] Boyer, M., Gelles, R., and Mor, T. (2012). Attacks on Fixed Apparatus Quantum Key Distribution Schemes. In *Proceedings of the 1<sup>st</sup> International Conference on Theory and Practice of Natural Computing*, pages 97–107. <http://www.cs.ucla.edu/~gelles/papers/BGM12.pdf>. 2.4.3
- [Brassard, 2005] Brassard, G. (2005). Brief History of Quantum Cryptography: A Personal Perspective. In *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, pages 19–23, Awaji Island, Japan. <http://arxiv.org/pdf/quant-ph/0604072v1.pdf>. 2.4.2
- [Brassard et al., 1994] Brassard, G. and Salvail, L. (1994). Secret-key Reconciliation by Public Discussion. In *Workshop on the theory and application of cryptographic techniques on Advances in Cryptology, EURO-CRYPT '93*, pages 410–423, Secaucus, NJ, USA. Springer-Verlag New York, Inc. 2.2.4
- [Brassard et al., 2000] Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.*, 85:1330–1333. <http://www.cs.technion.ac.il/~talmo/CV/my-papers/BLMS00pr1.pdf>. 2.4.1, 2.4.3, 6.2.2
- [Brown et al., 1986] Brown, R. G. W., Ridley, K. D., and Rarity, J. G. (1986). Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching. *Appl. Opt.*, 25(22):4122–4126. [ftp://ftp.artov.rm.cnr.it/incoming/ifa.rm.cnr.it/Maurizio.Viterbini/Public/apd/articoli/AQ/CA461B4C-BDB9-137E-C101D03BD78052D1\\_29835.pdf](ftp://ftp.artov.rm.cnr.it/incoming/ifa.rm.cnr.it/Maurizio.Viterbini/Public/apd/articoli/AQ/CA461B4C-BDB9-137E-C101D03BD78052D1_29835.pdf). 5.3.2
- [Brown et al., 1987] Brown, R. G. W., Jones, R., Rarity, J. G., and Ridley, K. D. (1987). Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching. *Appl. Opt.*, 26(12):2383–2389. [ftp://ftp.artov.rm.cnr.it/incoming/ifa.rm.cnr.it/Maurizio.Viterbini/Public/apd/articoli/AQ/CA43BCA9-BDB9-137E-C6BBCBDBB6C66E7E\\_30406.pdf](ftp://ftp.artov.rm.cnr.it/incoming/ifa.rm.cnr.it/Maurizio.Viterbini/Public/apd/articoli/AQ/CA43BCA9-BDB9-137E-C6BBCBDBB6C66E7E_30406.pdf). 5.3.2

- [Bruß, 1998] Bruß, D. (1998). Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett.*, 81:3018–3021. 2.2.1
- [Bruß et al., 2007] Bruß, D., Erdélyi, G., Meyer, T., Riege, T., and Rothe, J. (2007). Quantum cryptography: A survey. *ACM Comput. Surv.*, 39(2):1–31. <http://eccc.hpi-web.de/report/2005/146/revision/2/download>. 2.1.3
- [Buttler et al., 1998a] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M. (1998). Practical free-space quantum key distribution over 1 km. *arXiv:quant-ph/9805071*, pages 1–5. <http://arxiv.org/pdf/quant-ph/9805071.pdf>. 2.3.2, 2.5
- [Buttler et al., 1998b] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M. (1998). Free-space quantum-key distribution. *Phys. Rev. A*, 57:2379–2382. 2.3.2
- [Buttler et al., 2000] Buttler, W. T., Hughes, R. J., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G. (2000). Daylight Quantum Key Distribution over 1.6 km. *Phys. Rev. Lett.*, 84:5652–5655. <http://arxiv.org/pdf/quant-ph/0001088.pdf>. 2.5
- [Capraro, 2008] Capraro, I. (2008). *Advanced Techniques in Free Space Quantum Communication*. PhD thesis, Dipartimento di Ingegneria dell’Informazione. Università degli Studi di Padova. [http://paduaresearch.cab.unipd.it/615/1/phd\\_IvanCapraro.pdf](http://paduaresearch.cab.unipd.it/615/1/phd_IvanCapraro.pdf). 4.1.3
- [Capraro et al., 2008] Capraro, I., Occhipinti, T., Bonora, S., and Villoresi, P. (2008). Free Space Quantum Key Distribution System with Atmospheric Turbulence Mitigation by Active Deformable Mirror. In *Proceedings of the International Conference on Quantum Information*, page JMB64. Optical Society of America. 4.1.3
- [Cerf et al., 2001] Cerf, N. J., Lévy, M., and Assche, G. V. (2001). Quantum distribution of Gaussian keys using squeezed states. *Phys.*

- Rev.*, 63:052311–1–052311–5. <http://www.gva.noekeon.org/papers/2001-PRA-63-052311.pdf>. 2.2.1
- [Chapuran et al., 2009] Chapuran, T. E., Toliver, P., Peters, N. A., Jackel, J., Goodman, M. S., Runser, R. J., McNown, S. R., Dallmann, N., Hughes, R. J., McCabe, K. P., Nordholt, J. E., Peterson, C. G., Tyagi, K. T., Mercer, L., and Dardy, H. (2009). Optical networking for quantum key distribution and quantum communications. *New Journal of Physics*, 11(10):105001. [https://www.nsa.gov/research/\\_files/publications/qkd\\_networking\\_njp.pdf](https://www.nsa.gov/research/_files/publications/qkd_networking_njp.pdf). 4.1.3
- [Clarke et al., 2001] Clarke, R. B. M., Cheffles, A., Barnett, S. M., and Riis, E. (2001). Experimental demonstration of optimal unambiguous state discrimination. *Phys. Rev. A*, 63:040305. <http://arxiv.org/pdf/quant-ph/0007063v1>. 2.2.3, 2.4.3, 6.2, 6.2.2, 6.2.2
- [Clarke et al., 2011] Clarke, P. J., Collins, R. J., Hiskett, P. A., García-Martínez, M.-J., Krichel, N. J., McCarthy, A., Tanner, M. G., O’Connor, J. A., Natarajan, C. M., Miki, S., Sasaki, M., Wang, Z., Fujiwara, M., Rech, I., Ghioni, M., Gulinatti, A., Hadfield, R. H., Townsend, P. D., and Buller, G. S. (2011). Analysis of detector performance in a gigahertz clock rate quantum key distribution system. *New Journal of Physics*, 13(7):075008. (document), 1.1, 2.3.3, 5.3.1, 5.3.1
- [Clarke et al., 2012] Clarke, P. J., Collins, R. J., Dunjko, V., Andersson, E., Jeffers, J., and Buller, G. S. (2012). Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.*, 3:1174–1–1174–8. <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3493646/pdf/ncomms2172.pdf>. 2.2.2, 2.4.2
- [Claudon et al., 2010] Claudon, J., Bleuse, J., Malik, N. S., Bazin, M., Jaffrennou, P., Gregersen, N., Sauvan, C., Lalanne, P., and Geérard, J.-M. (2010). A highly efficient single-photon source based on a quantum dot in a photonic nanowire. *Nature Photonics*, 4:174–177. 3.3
- [Cobourne, 2011] Cobourne, S. (2011). Quantum Key Distribution Protocols and Applications. Technical Report RHUL–MA–2011–05,

- Department of Mathematics. Royal Holloway, University of London (UK). <http://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-05.pdf>. 2.1.3
- [Collins et al., 2007] Collins, R., Hadfield, R., Fernandez, V., Nam, S., and Buller, G. (2007). Low timing jitter detector for gigahertz quantum key distribution. *Electronic Letters*, 43:180–181. <http://arxiv.org/ftp/quant-ph/papers/0702/0702216.pdf>. 2.4.3, 5.3.1
- [Collins et al., 2010] Collins, R. J., Clarke, P. J., Fernández, V., Gordon, K. J., Makhonin, M. N., Timpson, J. A., Tahaoui, A., Hopkinson, M., and Fox, A. M. (2010). Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source. *Journal of Applied Physics*, 107:073102–073102–6. <http://arxiv.org/ftp/arxiv/papers/1004/1004.4754.pdf>. 3.3
- [Cova et al., 1991] Cova, S., Lacaita, A., and Ripamonti, G. (1991). Trapping phenomena in avalanche photodiodes on nanosecond scale. *Electron Device Letters, IEEE*, 12(12):685–687. <ftp://ftp.dei.polimi.it/users/Franco.Zappa/PDF/1991/IEEE%20EDL%201991.pdf>. 5.3
- [Cova et al., 1996] Cova, S., Ghioni, M., Lacaita, A., Samori, C., and Zappa, F. (1996). Avalanche photodiodes and quenching circuits for single-photon detection. *Applied Optics*, 35:1956–1976. <http://risorse.dei.polimi.it/spad/1996/App%200pt%201996.pdf>. 5.3.2
- [Dautet et al., 1993] Dautet, H., Deschamps, P., Dion, B., MacGregor, A. D., MacSween, D., McIntyre, R. J., Trottier, C., and Webb, P. P. (1993). Photon counting techniques with silicon avalanche photodiodes. *Appl. Opt.*, 32(21):3894–3900. <ftp://ftp.artov.rm.cnr.it/incoming/ifa.rm.cnr.it/Maurizio.Viterbini/Public/Lin/AvalanchePD2.pdf>. 5.3.1
- [Dianati et al., 2008] Dianati, M., Alléaume, R., Gagnaire, M., and Shen, X. (2008). Architecture and protocols of the future European quantum key distribution network. *Security and Communication Networks*, 1(1):57–74. 2.11

- [Diffie et al., 1976] Diffie, W. and Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654. 2.1.2
- [DTU, 2012] DTU (2012). VCSELs (last accessed dec. 2012). Technical report, Department of Photonic Engineering. Technical University of Denmark (DTU). [http://www.fotonik.dtu.dk/English/Research/ResearchActivities/NanoDevices\\_research/VCSELs.aspx](http://www.fotonik.dtu.dk/English/Research/ResearchActivities/NanoDevices_research/VCSELs.aspx). 3.3
- [Dušek et al., 2006] Dušek, M., Lütkenhaus, N., and Hendrych, M. (2006). Quantum cryptography. In *Progress in Optics Volume 49*, pages 381–454. Elsevier, New York (USA). <http://arxiv.org/pdf/quant-ph/0601207.pdf>. 2.4.3, 6.2.2
- [Ekert, 1991] Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.*, 67:661–663. 2.2.1, 2.4.4
- [Elser et al., 2009] Elser, D., Bartley, T., Heim, B., Wittmann, C., Sych, D., and Leuchs, G. (2009). Feasibility of free space quantum key distribution with coherent polarization states. *New Journal of Physics*, 11(4):045014. [http://iopscience.iop.org/1367-2630/11/4/045014/pdf/1367-2630\\_11\\_4\\_045014.pdf](http://iopscience.iop.org/1367-2630/11/4/045014/pdf/1367-2630_11_4_045014.pdf). 2.5
- [Erven et al., 2008a] Erven, C., Couteau, C., Laflamme, R., and Weihs, G. (2008). Entangled quantum key distribution over two free-space optical links. *Opt. Express*, 16(21):16840–16853. <http://www.opticsexpress.org/abstract.cfm?URI=oe-16-21-16840>. 2.5
- [Erven et al., 2008b] Erven, C., Couteau, C., Laflamme, R., and Weihs, G. (2008). Entanglement based free-space quantum key distribution. In *Proceedings of the SPIE 7099, Photonics North*, pages 709916–1–709916–7. <http://dx.doi.org/10.1117/12.807670>. 2.5
- [Erven et al., 2010] Erven, C., Hamel, D., Resch, K., Laflamme, R., and Weihs, G. (2010). Entanglement Based Quantum Key Distribution Using a Bright Sagnac Entangled Photon Source. In Sergienko, A., Pascazio, S., and Villoresi, P., editors, *Quantum Communication and Quantum Networking*, volume 36 of *Lecture Notes of the Institute for*

- Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 108–116. Springer, Berlin (Germany). 2.5
- [Fedrizzi et al., 2009] Fedrizzi, A., Ursin, R., Herbst, T., Nespoli, M., Prevedel, R., Scheidl, T., Tiefenbacher, F., Jennewein, T., and Zeilinger, A. (2009). High-fidelity transmission of entanglement over a high-loss freespace channel. *Nature Physics*, 5:389–392. <http://arxiv.org/pdf/0902.2015v2.pdf>. 2.5
- [Feng et al., 2007] Feng, Z., Ming-Xing, F., Yi-Qun, L., and Song-Hao, L. (2007). Influence of multi-photon pulses on practical differential-phase-shift quantum key distribution. *Chinese Physics*, 16(11):3402. 2.4.3
- [Fernández-Mármol, 2006] Fernández-Mármol, V. (2006). *Quantum Cryptography at High Speed*. PhD thesis, Heriot-Watt University, Edinburgh (U.K). 2.3.3
- [Friedlander et al., 1961] Friedlander, S. and Topper, L., editors (1961). *Turbulence, classic papers on statistical theory*. Interscience Publishers Inc., New York (USA). [http://www.ams.jhu.edu/~eyink/Turbulence/classics/Turbulence\\_Classic\\_Papers.pdf](http://www.ams.jhu.edu/~eyink/Turbulence/classics/Turbulence_Classic_Papers.pdf). 4.1.3
- [Fuchs et al., 1997] Fuchs, C. A., Gisin, N., Griffiths, R. B., Niu, C.-S., and Peres, A. (1997). Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Phys. Rev. A*, 56:1163–1172. 2.4.3
- [Fung et al., 2007] Fung, C.-H. F., Qi, B., Tamaki, K., and Lo, H.-K. (2007). Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A*, 75:032314. <http://arxiv.org/pdf/quant-ph/0601115v6.pdf>. 2.4.3
- [Fúster et al., 2012] Fúster, A., Hernández, L., Martín, A., Montoya, F., and Muñoz, J. (2012). *Criptografía, protección de datos y aplicaciones*. Rama, Madrid (Spain). 2.1.1, 2.1.2
- [García-Martínez et al., 2013] García-Martínez, M. J., Denisenko, N., Soto, D., Arroyo, D., Orue, A. B., and Fernandez, V. (2013). High-speed free-

- space quantum key distribution system for urban daylight applications. *Appl. Opt.*, 52(14):3311–3317. 6
- [García-Patrón, 2007] García-Patrón, R. (2007). *Quantum Information with Optical Continuous Variables : from Bell Tests to Key Distribution*. PhD thesis, Faculté des Sciences Appliquées. Université Libre de Bruxelles (Belgium). <http://theses.ulb.ac.be/ETD-db/collection/available/ULBetd-10022007-154607/unrestricted/Raul-Garcia-Patron-Thesis-2007.pdf>. 2.2.1
- [Gelles et al., 2012] Gelles, R. and Mor, T. (2012). On the security of interferometric quantum key distribution. In *Theory and Practice of Natural Computing*, volume 7505 of *Lecture Notes Comput. Sci.*, pages 133–146. Springer, Berlin (Germany). <http://arxiv.org/pdf/1110.6573.pdf>. 2.4.3
- [Gérard et al., 2004] Gérard, J. and Gayral, B. (2004). Toward high-efficiency quantum-dot single photon sources. In *Proceedings of SPIE 5361, Quantum Dots, Nanoparticles, and Nanoclusters*. <http://lib.semi.ac.cn:8080/tsh/dzzy/wsqq/SPIE/vol5361/5361-89.pdf>. 3.3
- [Gerhardt et al., 2011] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., and Makarov, V. (2011). Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.*, 2:349. <http://arxiv.org/pdf/1011.0105v2.pdf>. 2.4.3
- [Ghioni et al., 2003] Ghioni, M., Giudice, A., Cova, S., and Zappa, F. (2003). High-rate quantum key distribution at short wavelength: performance analysis and evaluation of silicon single photon avalanche diodes. *Journal of Modern Optics*, 50:2251–2269. <ftp://ftp.elet.polimi.it/outgoing/Franco.Zappa/PDF/2003/JM0%202003.pdf>. 5.3
- [Ghioni et al., 2009] Ghioni, M., Armellini, G., Maccagnani, P., Rech, I., Emley, M. K., and Ünlü, M. S. (2009). Resonant-cavity-enhanced single photon avalanche diodes on double silicon-on-insulator substrates. *Journal of Modern Optics*, 56(2-3):309–316. 5.3.1



- [Gisin et al., 1997] Gisin, N. and Huttner, B. (1997). Quantum cloning, eavesdropping and Bell's inequality. *Physics Letters A*, 232(6):463–476. <http://arxiv.org/pdf/quant-ph/9611041v1.pdf>. 2.4.3
- [Gisin et al., 2002] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum Cryptography. *Reviews of Modern Physics*, 74:145–195. <http://prl.aps.org/files/RevModPhys.74.145.pdf>. 2.3.1
- [Gisin et al., 2004] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N., and Scarani, V. (2004). Towards practical and fast quantum cryptography. *arXiv:quant-ph/0411022*, pages 1–7. <http://arxiv.org/pdf/quant-ph/0411022v1.pdf>. 2.2.1
- [Gisin et al., 2006] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G. (2006). Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73:022320. <http://arxiv.org/pdf/quant-ph/0507063v2.pdf>. 2.4.3
- [Gisin et al., 2010] Gisin, N., Pironio, S., and Sangouard, N. (2010). Proposal for Implementing Device-Independent Quantum Key Distribution based on a Heralded Qubit Amplification. *Phys. Rev. Lett.*, 105:070501. <http://arxiv.org/pdf/1003.0635v2.pdf>. 2.4.4
- [Gobby et al., 2004] Gobby, C., Yuan, Z. L., and Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84:3762–3764. <http://arxiv.org/ftp/quant-ph/papers/0412/0412171.pdf>. 2.3.2
- [Gordon et al., 2004] Gordon, K. J., Fernandez, V., Townsend, P. D., and Buller, G. S. (2004). A short wavelength GigaHertz clocked fiber-optic quantum key distribution system. *IEEE Journal of Quantum Electronics*, 40:900–908. <http://arxiv.org/ftp/quant-ph/papers/0605/0605222.pdf>. 3.3.2, 5.3.1
- [Gordon et al., 2005] Gordon, K., Fernandez, V., Buller, G., Rech, I., Cova, S., and Townsend, P. (2005). Quantum key distribution system clocked at 2 GHz. *Opt. Express*, 13(8):3015–3020. <http://arxiv.org/pdf/quant-ph/0605076>. 6.3.1

- [Gorman, 2010] Gorman, P. M. (2010). *Practical Free-Space Quantum Key Distribution*. PhD thesis, Department of Physics, Heriot-Watt University (UK). [http://www.ros.hw.ac.uk/bitstream/10399/2390/1/GormanPM\\_1210\\_eps.pdf](http://www.ros.hw.ac.uk/bitstream/10399/2390/1/GormanPM_1210_eps.pdf). 4.1.2
- [Gottesman et al., 2004] Gottesman, D., Lo, H.-K., Lütkenhaus, N., and Preskill, J. (2004). Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.*, 5:325–360. <http://arxiv.org/pdf/quant-ph/0212066v3.pdf>. 2.4.4, 6.2.2
- [Grabner et al., 2011] Grabner, M. and Kvicera, V. (2011). The wavelength dependent model of extinction in fog and haze for free space optical communication. *Opt. Express*, 19(4):3379–3386. 4.1.4
- [Grangier, 2006] Grangier, P. (2006). Experiments with single photons. In *Einstein, 1905–2005, Poincaré Seminar 2005. Progress in Mathematical Physics*, pages 1–26. Springer. <http://www.bourbaphy.fr/grangier.pdf>. 3.3
- [Grosshans et al., 2002] Grosshans, F. and Grangier, P. (2002). Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.*, 88:057902. 2.2.1
- [Guidetech, 2009] Guidetech (2009). GT658PCI Time Interval Analyzer. Last accessed March 2013. <http://www.guidetech.com/gallery/pc-based-instruments/gt658pci>. 5.4
- [Hadfield, 2009] Hadfield, R. H. (2009). Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3:696–705. [http://www.mba.ac.uk/pdf/EMB02011/le\\_photon\\_detectors\\_for\\_quantum\\_appl\\_Hadfield\\_Nat\\_Phot\\_2009%5B1%5D.pdf](http://www.mba.ac.uk/pdf/EMB02011/le_photon_detectors_for_quantum_appl_Hadfield_Nat_Phot_2009%5B1%5D.pdf). 5.3
- [Harrington et al., 2005] Harrington, J. W., Ettinger, J. M., Hughes, R. J., and Nordholt, J. E. (2005). Enhancing practical security of quantum key distribution with a few decoy states. *arXiv:quant-ph/0503002v1*, pages 1–4. <http://arxiv.org/pdf/quant-ph/0503002v1.pdf>. 2.4.3
- [Hastings et al., 2005] Hastings, S. R., de Dood, M. J. A., Kim, H., Marshall, W., Eisenberg, H. S., and Bouwmeester, D. (2005). Ultrafast

- optical response of a high-reflectivity GaAs/AlAs Bragg mirror. *Applied Physics Letters*, 86(3):031109. <http://web.physics.ucsb.edu/~quopt/ultra.pdf>. 3.3.1
- [Hecht, 2002] Hecht, E. (2002). *Optics*, 4<sup>th</sup> edition. Addison-Wesley. ISBN: 0-321-18878-0, San Francisco, CA (USA). 3.4
- [Heim et al., 2010] Heim, B., Elser, D., Bartley, T., Sabuncu, M., Wittmann, C., Sych, D., Marquardt, C., and Leuchs, G. (2010). Atmospheric channel characteristics for quantum communication with continuous polarization variables. *Applied Physics B*, 98:635–640. <http://arxiv.org/pdf/0910.4543v2.pdf>. 2.5
- [Hiskett et al., 2001] Hiskett, P. A., Bonfrate, G., Buller, G. S., and Townsend, P. D. (2001). Eighty kilometre transmission experiment using an In-GaAs/InP SPAD-based quantum cryptography receiver operating at 1.55  $\mu\text{m}$ . *Journal of Modern Optics*, 48(13):1957–1966. <http://pcg.eps.hw.ac.uk/publications/journals/jmo-48-13-1957.pdf>. 5.3
- [Hong et al., 1986] Hong, C. K. and Mandel, L. (1986). Experimental realization of a localized one-photon state. *Phys. Rev. Lett.*, 56:58–60. 2.3.1
- [Honjo et al., 2009] Honjo, T., Uchida, A., Amano, K., Hirano, K., Someya, H., Okumura, H., Yoshimura, K., Davis, P., and Tokura, Y. (2009). Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers. *Opt. Express*, 17(11):9053–9061. <http://www.opticsexpress.org/abstract.cfm?URI=oe-17-11-9053>. 2.4.2
- [Houghton, 1986] Houghton, J. T. (1986). *The Physics of Atmospheres*, 2<sup>nd</sup> Ed. Cambridge University Press. ISBN-10: 0521327318, Cambridge (UK). 4.1.3
- [Hughes et al., 1999] Hughes, R. J., Morgan, G. L., and Peterson, C. G. (1999). Practical quantum key distribution over a 48-km optical fiber network. Technical Report LA-UR-99-1593, Los Alamos National Laboratory (USA). <http://arxiv.org/ftp/quant-ph/papers/9904/9904038.pdf>. 2.3.2

- [Hughes et al., 2000] Hughes, R. J., Buttler, W. T., Kwiat, P. G., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G. (2000). Free-space quantum key distribution in daylight. *Journal of Modern Optics*, 47(2-3):549–562. 2.3.2
- [Hughes et al., 2002a] Hughes, R., Nordholt, J. E., Morgan, G. L., and Peterson, C. G. (2002). Free space quantum key distribution over 10 km in daylight and at night. In *Nonlinear Optics: Materials, Fundamentals and Applications*, page FA2. 2.5
- [Hughes et al., 2002b] Hughes, R. J., Nordholt, J. E., Derkacs, D., and Peterson, C. G. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4(1):43. <http://arxiv.org/ftp/quant-ph/papers/0206/0206092.pdf>. 2.5, 4.1.5, 5.8, 6.3.4
- [Huttner et al., 1995] Huttner, B., Imoto, N., Gisin, N., and Mor, T. (1995). Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869. <http://arxiv.org/pdf/quant-ph/9502020v1.pdf>. 2.4.3, 6.2.2
- [Hwang, 2003] Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901. <http://arxiv.org/pdf/quant-ph/0211153v5.pdf>. 2.3.1, 2.4.3
- [IDQ, 2012] IDQ (2012). id100 series IDQ Datasheet. Last accessed March 2013. <http://www.idquantique.com/images/stories/PDF/id100-single-photon-detector/id100-specs.pdf>. 5.3.1
- [Iga et al., 1987] Iga, K., Kinoshita, S., and Koyama, F. (1987). Microcavity *GaAlaAs/GaAs* surface-emitting laser with  $I_{th} = 6$  mA. *Electronics Letters*, 23(3):134–136. 3.3.1
- [Inoue et al., 2002] Inoue, K., Waks, E., and Yamamoto, Y. (2002). Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89:037902. <http://prl.aps.org/pdf/PRL/v89/i3/e037902>. 2.2.1, 2.4.3
- [Inoue et al., 2003] Inoue, K., Waks, E., and Yamamoto, Y. (2003). Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A*, 68:022317. 2.2.1

- [Ivanovic, 1987] Ivanovic, I. (1987). How to differentiate between non-orthogonal states. *Physics Letters A*, 123(6):257–259. 2.2.3
- [Jacobs et al., 1996] Jacobs, B. C. and Franson, J. D. (1996). Quantum cryptography in free space. *Opt. Lett.*, 21:1854–1856. 2.3.2
- [Jain et al., 2011a] Jain, N., Lydersen, L., Wittmann, C., Wiechers, C., Elser, D., Marquardt, C., Makarov, V., and Leuchs, G. (2011). Inducing a detector efficiency mismatch to hack a commercial quantum key distribution system. In *Proceedings of CLEO/Europe-EQEC 2011*, Munich (Germany). [http://www.vad1.com/publications/CLEO\\_Europe\\_EQEC\\_2011-Jain.pdf](http://www.vad1.com/publications/CLEO_Europe_EQEC_2011-Jain.pdf). 2.4.4
- [Jain et al., 2011b] Jain, N., Wittmann, C., Lydersen, L., Wiechers, C., Elser, D., Marquardt, C., Makarov, V., and Leuchs, G. (2011). Device Calibration Impacts Security of Quantum Key Distribution. *Phys. Rev. Lett.*, 107:110501. 2.4.3
- [Jewell et al., 1991] Jewell, J., Harbison, J., Scherer, A., Lee, Y., and Florez, L. (1991). Vertical-cavity surface-emitting lasers: Design, growth, fabrication, characterization. *IEEE Journal of Quantum Electronics*, 27(6):1332–1346. 3.3.1
- [Kim et al., 2001a] Kim, I. I. and Korevaar, E. J. (2001). Availability of free-space optics (FSO) and hybrid FSO/RF systems. In *Proceedings of SPIE 4530, Optical Wireless Communications IV*, pages 84–95. <http://www.ece.mcmaster.ca/~hranilovic/woc/resources/local/spie2001b.pdf>. 4.1.4
- [Kim et al., 2001b] Kim, I. I., McArthur, B., and Korevaar, E. J. (2001). Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. In *Proceedings of SPIE 4214, Optical Wireless Communications III*, pages 26–37. [http://www.lightpointe.com/images/LightPointe\\_historical\\_Free\\_Space\\_Optics\\_info\\_Comparison\\_of\\_laser\\_beam\\_propagation\\_MRV\\_7.pdf](http://www.lightpointe.com/images/LightPointe_historical_Free_Space_Optics_info_Comparison_of_laser_beam_propagation_MRV_7.pdf). 4.1.4

- [Koashi, 2004] Koashi, M. (2004). Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse. *Phys. Rev. Lett.*, 93:120501. 2.2.3
- [Kolmogorov, 1941] Kolmogorov, A. N. (1941). The local structure of turbulence in an incompressible viscous fluid for very large Reynolds numbers. *C. R. (Doki) Acad. Sci. U.S.S.R.*, 30:301–305. [http://www.astro.puc.cl/~rparra/tools/PAPERS/kolmogorov\\_1951.pdf](http://www.astro.puc.cl/~rparra/tools/PAPERS/kolmogorov_1951.pdf). 4.1.3
- [Kurtsiefer et al., 2001] Kurtsiefer, C., Zarda, P., Mayer, S., and Weinfurter, H. (2001). The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? *Journal of Modern Optics*, 48(13):2039–2047. [http://xqp.physik.uni-muenchen.de/publications/files/articles\\_2001/journmodopt\\_48\\_2039.pdf](http://xqp.physik.uni-muenchen.de/publications/files/articles_2001/journmodopt_48_2039.pdf). 2.4.3
- [Kurtsiefer et al., 2002] Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R., and Rarity, J. G. (2002). Quantum cryptography: A step towards global key distribution. *Nature*, 419:450. 2.5
- [Kwiat et al., 1995] Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V., and Shih, Y. (1995). New High-Intensity Source of Polarization-Entangled Photon Pairs. *Phys. Rev. Lett.*, 75:4338–4341. <http://people.bu.edu/alexserg/Entangled.pdf>. 2.3.1
- [Lamas-Linares et al., 2007] Lamas-Linares, A. and Kurtsiefer, C. (2007). Breaking a quantum key distribution system through a timing side channel. *Opt. Express*, 15(15):9388–9393. <http://arxiv.org/pdf/0704.3297v2.pdf>. 2.4.3
- [Levine et al., 1984] Levine, B. and Bethea, C. (1984). Single-photon detection at 1.3  $\mu\text{m}$  using a gated avalanche photodiode. *Applied Physics Letters*, 44(5):553–555. 5.3.2
- [Li et al., 2007] Li, Y., Hua, S., Liu, Y., Ye, J., and Zhou, Q. (2007). Quantum repeaters: fundamental and future. In *Proceedings of SPIE. 6573, Quantum Information and Computation*. <http://sites.google.com/site/xyly781/7.PSI65730XQuantumrepeatersfundament.pdf>. 2.3.2

- [Lo et al., 1999] Lo, H.-K. and Chau, H. F. (1999). Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056. <http://arxiv.org/pdf/quant-ph/9803006v5.pdf>. 2.4.2
- [Lo et al., 2005] Lo, H.-K., Ma, X., and Chen, K. (2005). Decoy State Quantum Key Distribution. *Phys. Rev. Lett.*, 94:230504. <http://arxiv.org/pdf/quant-ph/0411004>. 2.3.1
- [Lucamarini et al., 2009] Lucamarini, M., Di Giuseppe, G., and Tamaki, K. (2009). Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states. *Phys. Rev. A*, 80:032327. 3.3, 6.3.2
- [Lütkenhaus, 2000] Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61:052304–1–052304–10. <http://arxiv.org/pdf/quant-ph/9910093v2.pdf>. 2e, 2.3.1, 2.4.1, 6.3.2
- [Lütkenhaus et al., 2002] Lütkenhaus, N. and Jahma, M. (2002). Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44. <http://arxiv.org/pdf/quant-ph/0112147v1.pdf>. 2.4.3
- [Lydersen et al., 2010a] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689. <http://arxiv.org/pdf/1008.4593.pdf>. 2.4.3, 2.4.3, 2.4.4
- [Lydersen et al., 2010b] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V. (2010). Thermal blinding of gated detectors in quantum cryptography. *Opt. Express*, 18(26):27938–27954. <http://arxiv.org/pdf/1009.2663v1.pdf>. 2.4.3
- [Lydersen, 2011] Lydersen, L. V. (2011). *Practical Security of Quantum Cryptography*. PhD thesis, Faculty of Information Technology, Mathematics and Electrical Engineering. Norwegian University of Science

- and Technology, Trondheim (Norway). <http://www.vad1.com/lab/publications/Lydersen-PhD-thesis-20110919.pdf>. 2.4.3, 2
- [Lydersen et al., 2011a] Lydersen, L., Jain, N., Wittmann, C., Marøy, O., Skaar, J., Marquardt, C., Makarov, V., and Leuchs, G. (2011). Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A*, 84:032320. <http://arxiv.org/pdf/1106.2119v2.pdf>. 2.4.3
- [Lydersen et al., 2011b] Lydersen, L., Makarov, V., and Skaar, J. (2011). Secure gated detection scheme for quantum cryptography. *Phys. Rev. A*, 83:032306. <http://arxiv.org/pdf/1101.5698v1.pdf>. 2.4.3
- [Ma, 2008] Ma, X. (2008). *Quantum cryptography: from theory to practice*. PhD thesis, Department of Physics. University of Toronto (Canada). [https://tspace.library.utoronto.ca/bitstream/1807/17302/1/Ma\\_Xiongfeng\\_200811\\_\\_PhD\\_thesis.pdf](https://tspace.library.utoronto.ca/bitstream/1807/17302/1/Ma_Xiongfeng_200811__PhD_thesis.pdf). 2.5
- [Ma et al., 2007] Ma, X., Fung, C.-H. F., and Lo, H.-K. (2007). Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307. <http://arxiv.org/pdf/quant-ph/0703122v1.pdf>. 2.5
- [Makarov et al., 2005] Makarov, V. and Hjelme, D. R. (2005). Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 52:691–705. 2.4.3
- [Makarov et al., 2006] Makarov, V., Anisimov, A., and Skaar, J. (2006). Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74:022313. <http://www.vad1.com/publications/PhysRevA-74-022313-and-erratum-PhysRevA-78-019905.pdf>. 2.4.3, 2.12
- [Makarov et al., 2008] Makarov, V. and Skaar, J. (2008). Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Information and Computation*, 8:0622–0635. <http://www.vad1.com/publications/QuantInfComp-8-0622.pdf>. 2.4.3



- [Makarov et al., 2009] Makarov, V., Anisimov, A., and Sauge, S. (2009). Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve. *arXiv:0809.3408v2 [quant-ph]*, pages 1–4. <http://arxiv.org/pdf/0809.3408v2.pdf>. 2.4.3
- [Mansuripur, 2002] Mansuripur, M. (2002). *Classical Optics and Its Applications*. Cambridge University Press. ISBN: 0 521 80093 5, Cambridge (UK). 2.4.1
- [Marcikic et al., 2006] Marcikic, I., Lamas-Linares, A., and Kurtsiefer, C. (2006). Free-space quantum key distribution with entangled photons. *Applied Physics Letters*, 89(10):101122. <http://arxiv.org/pdf/quant-ph/0606072v2.pdf>. 2.5
- [Martínez-Mateo, 2008] Martínez-Mateo, J. (2008). Criptografía cuántica aplicada. Master’s thesis, Facultad de Informática. Universidad Politécnica de Madrid (Spain). 2.2.1
- [Martínez-Mateo et al., 2010] Martínez-Mateo, J., Elkouss, D., and Martín, V. (2010). Interactive reconciliation with low-density parity-check codes. In *Proceedings of the 6<sup>th</sup> Turbo Codes and Iterative Information Processing (ISTC)*, pages 270–274. <http://arxiv.org/pdf/1006.4484.pdf>. 6.2.2
- [Mayers, 2001] Mayers, D. (2001). Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406. <http://arxiv.org/ftp/quant-ph/papers/9802/9802025.pdf>. 2.4.2
- [Mayers et al., 1998] Mayers, D. and Yao, A. (1998). Quantum cryptography with imperfect apparatus. In *Proceedings of 39<sup>th</sup> Annual Symposium on Foundations of Computer Science*, pages 503–509. <http://arxiv.org/pdf/quant-ph/9809039.pdf>. 2.4.4
- [McDonough, 2004] McDonough, J. M. (2004). Introductory lectures on turbulence. Physics, Mathematics and Modeling. Technical report, Departments of Mechanical Engineering and Mathematics. University of Kentucky (USA). <http://www.engr.uky.edu/~acfd/lctr-notes634.pdf>. 4.1.3

- [Meade, 2003] Meade (2003). *8", 10", 12", 14", 16" LX200GPS Schmidt-Cassegrain Telescopes Instruction Manual*. Meade Instruments Corporation. 4.7, 4.2.2
- [Menzel, 2007] Menzel, R. (2007). *Photonics. Linear and Nonlinear Interactions of Laser Light and Matter, 2<sup>nd</sup> edition*. Springer, Berlin. ISBN: 978-3-540-23160-8, Berlin, (Germany). <http://lib.semi.ac.cn:8080/tsh/dzzy/ebooks/full/fn331.pdf>. 4.2.1, 4.2.1
- [Meyer-Scott et al., 2011] Meyer-Scott, E., Yan, Z., MacDonald, A., Bourgoin, J.-P., Hübel, H., and Jennewein, T. (2011). How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss. *Phys. Rev. A*, 84:062326. <http://arxiv.org/pdf/1111.0976v2>. 2.5
- [Miki et al., 2008] Miki, S., Fujiwara, M., Sasaki, M., Baek, B., Miller, A. J., Hadfield, R. H., Nam, S. W., and Wang, Z. (2008). Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates. *Applied Physics Letters*, 92(6):061116. 5.3.1
- [Mikulevicius et al., 2004] Mikulevicius, R. and Rozovskii, B. (2004). Stochastic Navier–Stokes Equations for Turbulent Flows. *SIAM Journal on Mathematical Analysis*, 35(5):1250–1310. <http://www.ima.umn.edu/prob-pde/reprints-preprints/rozovskii/NSESIAM7IMA.pdf>. 4.1.3
- [MPD, 2012] MPD (2012). PDM series Micro Photon Devices Datasheet v3.8. Last accessed March 2013. <http://www.micro-photon-devices.com/media/pdf/PDM.pdf>. 5.3.1
- [Muller et al., 1997] Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., and Gisin, N. (1997). Plug and play systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795. <http://arxiv.org/pdf/quant-ph/9611042v1.pdf>. 2.4.3
- [Nauerth et al., 2013] Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S., and Weinfurter, H. (2013). Air-to-ground quantum communication. *Nature Photonics*, 7:382–386. 2.5

- [Peev et al., 2009] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J. F., Fasel, S., Fossier, S., Fürst, M., Gautier, J.-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hübel, H., Humer, G., Länger, T., Legré, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J.-B., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A. W., Shields, A. J., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R. T., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Brouri, R., Vannel, F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z. L., Zbinden, H., and Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11(7):075001. [http://iopscience.iop.org/1367-2630/11/7/075001/pdf/1367-2630\\_11\\_7\\_075001.pdf](http://iopscience.iop.org/1367-2630/11/7/075001/pdf/1367-2630_11_7_075001.pdf). 2.5
- [Peloso et al., 2009] Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A., and Kurtsiefer, C. (2009). Daylight operation of a free space, entanglement-based quantum key distribution system. *New Journal of Physics*, 11(4):045007. [http://iopscience.iop.org/1367-2630/11/4/045007/pdf/1367-2630\\_11\\_4\\_045007.pdf](http://iopscience.iop.org/1367-2630/11/4/045007/pdf/1367-2630_11_4_045007.pdf). 2.5, 5.8
- [PerkinElmer, 2005] PerkinElmer (2005). SPCM-AQR single photon counting module Perkin Elmer Datasheet. Last accessed March 2013. <http://www.scitecinstruments.pl/detektory/pcm/pdf/SPCMAQR.pdf>. 5.3.1, 5.3.3
- [Pfennigbauer et al., 2005] Pfennigbauer, M., Aspelmeyer, M., Leeb, W. R., Baister, G., Dreischer, T., Jennewein, T., Neckamm, G., Perdigues, J. M., Weinfurter, H., and Zeilinger, A. (2005). Satellite-based quantum communication terminal employing state-of-the-art technology. *Journal of Optical Networking*, 4:549–560. [http://publik.tuwien.ac.at/files/pub-et\\_9816.pdf](http://publik.tuwien.ac.at/files/pub-et_9816.pdf). 2.5
- [Pironio et al., 2009] Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., and Scarani, V. (2009). Device-independent quantum key distribution secure against collective attacks. *New Journal of*

- Physics*, 11(4):045021. [http://iopscience.iop.org/1367-2630/11/4/045021/pdf/1367-2630\\_11\\_4\\_045021.pdf](http://iopscience.iop.org/1367-2630/11/4/045021/pdf/1367-2630_11_4_045021.pdf). 2.4.4
- [Qi et al., 2007] Qi, B., Fung, C.-H. F., Lo, H.-K., and Ma, X. (2007). Time-shift attack in practical quantum cryptosystems. *Quantum Info. Comput.*, 7(1):73–82. <http://arxiv.org/pdf/quant-ph/0512080v3.pdf>. 2.4.3
- [Radenbaugh, 2004] Radenbaugh, R. (2004). Refrigeration for superconductors. *Proceedings of the IEEE*, 92(10):1719–1734. 5.3.1
- [Rarity et al., 2001] Rarity, J., Gorman, P., and Tapster, P. (2001). Secure key exchange over 1.9 km free-space range using quantum cryptography. *Electronics Letters*, 37:512–514. 2.5
- [Resch et al., 2005] Resch, K., Lindenthal, M., Blauensteiner, B., Böhm, H., Fedrizzi, A., Kurtsiefer, C., Poppe, A., Schmitt-Manderbach, T., Taraba, M., Ursin, R., Walther, P., Weier, H., Weinfurter, H., and Zeilinger, A. (2005). Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Opt. Express*, 13(1):202–209. <http://arxiv.org/ftp/quant-ph/papers/0501/0501008.pdf>. 2.5
- [Rech et al., 2006] Rech, I., Labanca, I., Ghioni, M., and Cova, S. (2006). Modified single photon counting modules for optimal timing performance. *Review of Scientific Instruments*, 77(3):033104. 5.3.1
- [Restelli et al., 2010] Restelli, A., Bienfang, J., Clark, C., Rech, I., Labanca, I., Ghioni, M., and Cova, S. (2010). Improved Timing Resolution Single-Photon Detectors in Daytime Free-Space Quantum Key Distribution With 1.25 GHz Transmission Rate. *IEEE Journal of Selected Topics in Quantum Electronics*, 16(5):1084–1090. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5433021>. 2.5, 5.3.1
- [Rivest et al., 1978] Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126. 2.1.2

- [Safari et al., 2009] Safari, M. and Uysal, M. (2009). Relay-assisted quantum-key distribution over long atmospheric channels. *J. Lightwave Technol.*, 27(20):4508–4515. <http://faculty.ozyegin.edu.tr/muratuysal/files/2011/05/J41.pdf>. 4.1.3
- [Saleh et al., 2007] Saleh, B. E. A. and Teich, M. C. (2007). *Fundamentals of Photonics, 2<sup>nd</sup> Edition*. Wiley Interscience, ISBN 0-471-83965-5, New Jersey (USA). 5.3.2, 5.4
- [Salomon, 2006] Salomon, D. (2006). *Foundations of Computer Security*. Springer. ISBN: 978-1-84628-341-3, Berlin (Germany). <http://link.springer.com/book/10.1007/1-84628-341-8/page/1>. 2.1
- [Sauge et al., 2011] Sauge, S., Lydersen, L., Anisimov, A., Skaar, J., and Makarov, V. (2011). Controlling an actively-quenched single photon detector with bright light. *Opt. Express*, 19(23):23590–23600. <http://www.vad1.com/publications/OptExpress-19-23590.pdf>. 2.4.3
- [Scarani et al., 2004] Scarani, V., Acín, A., Ribordy, G., and Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901. <http://www.icfo.es/images/publications/C03-001.pdf>. 2.2.1, 2.4.3
- [Scarani et al., 2009a] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350. [http://www.physics.nus.edu.sg/corporate/research/res\\_paper/RevModPhys\\_81\\_001301.pdf](http://www.physics.nus.edu.sg/corporate/research/res_paper/RevModPhys_81_001301.pdf). 2.2.1, 2.4.4
- [Scarani et al., 2009b] Scarani, V. and Kurtsiefer, C. (2009). The black paper of quantum cryptography: real implementation problems. *arXiv:0906.4547v2 [quant-ph]*, pages 1–6. <http://arxiv.org/pdf/0906.4547v2.pdf>. 2.4.2
- [Scheidl et al., 2009] Scheidl, T., Ursin, R., Fedrizzi, A., Ramelow, S., Ma, X.-S., Herbst, T., Prevedel, R., Ratschbacher, L., Kofler, J., Jennewein, T., and Zeilinger, A. (2009). Feasibility of 300 km

- quantum key distribution with entangled states. *New Journal of Physics*, 11(8):085002. [http://iopscience.iop.org/1367-2630/11/8/085002/pdf/1367-2630\\_11\\_8\\_085002.pdf](http://iopscience.iop.org/1367-2630/11/8/085002/pdf/1367-2630_11_8_085002.pdf). 2.5
- [Scherer et al., 2011] Scherer, A., Sanders, B. C., and Tittel, W. (2011). Long-distance practical quantum key distribution by entanglement swapping. *Optics Express*, 19:3004–3018. <http://arxiv.org/pdf/1012.5675.pdf>. 2.3.2
- [Schmitt-Manderbach, 2007] Schmitt-Manderbach, T. (2007). Long distance free-space quantum key distribution. Master’s thesis, Faculty of Physics of the Ludwig–Maximilians–Universität München (Germany). [http://edoc.ub.uni-muenchen.de/8102/1/Schmitt-Manderbach\\_Tobias.pdf](http://edoc.ub.uni-muenchen.de/8102/1/Schmitt-Manderbach_Tobias.pdf). 4.1.2
- [Schmitt-Manderbach et al., 2007] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A., and Weinfurter, H. (2007). Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.*, 98:010504. <http://prl.aps.org/pdf/PRL/v98/i1/e010504>. (document), 1.1, 2.5
- [Self, 1983] Self, S. A. (1983). Focusing of spherical Gaussian beams. *Appl. Opt.*, 22(5):658–661. [http://homepages.cae.wisc.edu/~ssanders/me\\_770/journal\\_papers/Self\\_1983\\_focusing\\_gaussian\\_beams\\_AWC.pdf](http://homepages.cae.wisc.edu/~ssanders/me_770/journal_papers/Self_1983_focusing_gaussian_beams_AWC.pdf). 4.2.3
- [Sergienko, 2006] Sergienko, A. V., editor (2006). *Quantum Communications and Cryptography*. CRC Taylor & Francis. ISBN: 0-8493-3684-8, Boca Raton, FL (USA). 2.1
- [Shannon, 1948] Shannon, C. E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27:379–423 and 623–656. <http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf>. 2.1
- [Shannon, 1949a] Shannon, C. (1949). Communication in the Presence of Noise. *Proceedings of the IRE (Reprinted: Proceedings of the IEEE, 86,*

- No. 2, 1998*)., 37:10–21. <http://www.ccs.neu.edu/course/csg250/ShannonNoise.pdf>. 2.2.4
- [Shannon, 1949b] Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28:656–715. <http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf>. 2.1
- [Shor, 1994] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35<sup>th</sup> Annual Symposium on Foundations of Computer Science*, SFCS '94, pages 124–134, Washington, DC, USA. [http://www.csee.wvu.edu/~xinl/library/papers/comp/shor\\_focs1994.pdf](http://www.csee.wvu.edu/~xinl/library/papers/comp/shor_focs1994.pdf). 2.4.2
- [Shor, 1997] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509. <http://arxiv.org/pdf/quant-ph/9508027v2.pdf>. 2.1.3
- [Shor et al., 2000] Shor, P. W. and Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441. <http://arxiv.org/pdf/quant-ph/0003004v2.pdf>. 2.4.2
- [Siegman, 1971] Siegman, A. E. (1971). *An introduction to lasers and masers*. McGraw-Hill. ISBN: 007057362X, New York (USA). 4.2.3
- [Silberhorn et al., 2002] Silberhorn, C., Ralph, T. C., Lütkenhaus, N., and Leuchs, G. (2002). Continuous Variable Quantum Cryptography: Beating the 3~dB Loss Limit. *Phys. Rev. Lett.*, 89:167901. 2.2.1
- [Singh, 1999] Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books - Random House, Inc. ISBN: 0385495323, New York (USA). 2.1
- [Smith, 2000] Smith, W. J. (2000). *Modern Optical Engineering. The Design of Optical Systems*, 3<sup>rd</sup> Ed. McGraw-Hill. ISBN: 0-07-136360-2, New York (USA). 4.2.3
- [Smith et al., 2007] Smith, F. G., King, T. A., and Wilkins, D. (2007). *Optics and Photonics: An Introduction*, 2<sup>nd</sup> edition. John Wiley & Sons, Ltd. ISBN: 978-0-470-01784-5, West Sussex (UK). 3.3.1



- [Stucki et al., 2001] Stucki, D., Ribordy, G., Stefanov, A., Zbinden, H., Rarity, J. G., and Wall, T. (2001). Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs. *Journal of Modern Optics*, 48:1967–1981. <http://arxiv.org/pdf/quant-ph/0106007v1>. 2.3.2, 5.3
- [Stucki et al., 2005] Stucki, D., Brunner, N., Gisin, N., Scarani, V., and Zbinden, H. (2005). Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.*, 87:194108. 2.2.1
- [Stucki et al., 2009] Stucki, D., Walenta, N., Vannel, F., Thew, R. T., Gisin, N., Zbinden, H., Gray, S., Tower, C. R., and Ten, S. (2009). High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003. [http://iopscience.iop.org/1367-2630/11/7/075003/pdf/1367-2630\\_11\\_7\\_075003.pdf](http://iopscience.iop.org/1367-2630/11/7/075003/pdf/1367-2630_11_7_075003.pdf). 2.3.2
- [Sun et al., 2011] Sun, S.-H., Jiang, M.-S., and Liang, L.-M. (2011). Passive faraday mirror attack in practical two-way quantum key distribution system. *Phys. Rev. A*, 83:062331. <http://arxiv.org/pdf/1203.0739v1.pdf>. 2.4.3
- [Takesue et al., 2007] Takesue, H., Nam, S. W., Zhang, Q., Hadfield, R. H., Honjo, T., Tamaki, K., and Yamamoto, Y. (2007). Quantum key distribution over 40 dB channel loss using superconducting single photon detectors. *Nature Photonics*, 1:343–348. <http://arxiv.org/pdf/0706.0397v1>. 5.3.1
- [Tamaki et al., 2003] Tamaki, K., Koashi, M., and Imoto, N. (2003). Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. *Phys. Rev. A*, 67:032310. <http://arxiv.org/pdf/quant-ph/0212161v1.pdf>. 2.2.3, 2.4.3, 6.2.2
- [Tamaki et al., 2004] Tamaki, K. and Lütkenhaus, N. (2004). Unconditional Security of the Bennett 1992 quantum key-distribution over lossy and noisy channel. *Phys. Rev. A*, 69:032316. <http://arxiv.org/pdf/quant-ph/0308048v2.pdf>. 2.2.3



- [Tamaki et al., 2009] Tamaki, K., Lütkenhaus, N., Koashi, M., and Batuwantudawe, J. (2009). Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse. *Phys. Rev. A*, 80:032302. <http://arxiv.org/pdf/quant-ph/0607082v2.pdf>. 2.2.3
- [Tanaka et al., 2008] Tanaka, A., Fujiwara, M., Nam, S. W., Nambu, Y., Takahashi, S., Maeda, W., ichiro Yoshino, K., Miki, S., Baek, B., Wang, Z., Tajima, A., Sasaki, M., and Tomita, A. (2008). Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Opt. Express*, 16(15):11354–11360. <http://arxiv.org/pdf/0805.2193v2>. 5.3.1
- [Tang et al., 2009] Tang, X., Ma, L., Mink, A., Nakassis, A., Hershman, B., Bienfang, J., Boisvert, R. F., Clark, C., and Williams, C. (2009). High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding. *CiteSeerX—Scientific Literature Digital Library and Search Engine (United States)*, 1<sup>st</sup> version in *Proceedings of SPIE*, vol. 5893, *Optics and Photonics*, pages 1–9. [http://w3.antd.nist.gov/pubs/SPIE\\_final-fiber-polarization.pdf](http://w3.antd.nist.gov/pubs/SPIE_final-fiber-polarization.pdf). 2.3.2
- [Temporao et al., 2008] Temporao, G., Zbinden, H., Tanzilli, S., Gisin, N., Aellen, T., Giovannini, M., Faist, J., and von der Weid, J. (2008). Feasibility study of free-space quantum key distribution in the mid-infrared. *Quantum Info. Comput.*, 8(1):1–11. [http://www.gap-optics.unige.ch/wiki/\\_media/publications:bib:qic-guilherme.pdf](http://www.gap-optics.unige.ch/wiki/_media/publications:bib:qic-guilherme.pdf). 2.5
- [Toyoshima et al., 2008] Toyoshima, M., Takayama, Y., Klaus, W., Kunimori, H., Fujiwara, M., and Sasaki, M. (2008). Free-space quantum cryptography with quantum and telecom communication channels. *Acta Astronautica*, 63:179–184. <http://www.sciencedirect.com/science/article/pii/S0094576507003372>. 2.5
- [Tunick et al., 2010] Tunick, A., Moore, T., Deacon, K., and Meyers, R. (2010). Review of representative free-space quantum communications experiments. In *Proceedings of SPIE 7815, Quantum Communications and Quantum Imaging VIII*, pages 781512–781512–10. 2.5

- [Uchiyama et al., 1985] Uchiyama, S. and Iga, K. (1985). Two-dimensional array of GaInAsP/InP surface-emitting lasers. *Electronics Letters*, 21(4):162–164. 3.3.1
- [Ursin et al., 2007] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., H.Weier, Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., and Zeilinger, A. (2007). Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481–486. [http://homepage.univie.ac.at/rupert.ursin/php/?download=2007-entangled\\_tenerife.pdf](http://homepage.univie.ac.at/rupert.ursin/php/?download=2007-entangled_tenerife.pdf). 2.5
- [Vakhitov et al., 2001] Vakhitov, A., Makarov, V., and Hjelme, D. R. (2001). Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48:2023–2038. <http://www.iet.ntnu.no/groups/optics/qcr/paper-vakhitov-2001/paper-vakhitov-2001.pdf>. 2.4.3
- [Vandersypen et al., 2001] Vandersypen, L., Steffen, M., Breyta, G., Yannoni, C., Sherwood, M., and Chuang, I. (2001). Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883–887. <http://cryptome.org/shor-nature.pdf>. 2.1.3
- [Vazirani et al., 2012] Vazirani, U. and Vidick, T. (2012). Fully device independent quantum key distribution. *arXiv:1210.1810 [quant-ph]*. <http://arxiv.org/pdf/1210.1810v2.pdf>. 2.4.4
- [Vernam, 1919] Vernam, G. S. (1919). *Secret Signaling System*. United States Patent Office. Specification of Letters Patent. 2.1
- [Vernam, 1926] Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*, XLV:295–301. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5061224>. (document), 1.1
- [Villoresi et al., 2008] Villoresi, P., Jennewein, T., Tamburini, F., Aspelmeyer, M., Bonato, C., Ursin, R., Pernechele, C., Luceri, V., Bianco, G.,

- Zeilinger, A., and Barbieri, C. (2008). Experimental verification of the feasibility of a quantum channel between space and earth. *New Journal of Physics*, 10(3):033038. [http://iopscience.iop.org/1367-2630/10/3/033038/pdf/1367-2630\\_10\\_3\\_033038.pdf](http://iopscience.iop.org/1367-2630/10/3/033038/pdf/1367-2630_10_3_033038.pdf). 2.5
- [Wallace et al., 2006] Wallace, J. M. and Hobbs, P. V. (2006). *Atmospheric Science. An Introductory Survey*. Elsevier. 4.1.3
- [Wang, 2006] Wang, X.-B. (2006). Quantum Key Distribution: Security, Feasibility and Robustness. In Imai, H. and Hayashi, M., editors, *Quantum Computation and Information*, volume 102 of *Topics in Applied Physics*, pages 185–233. Springer, Berlin (Germany). [http://link.springer.com/content/pdf/10.1007%2F3-540-33133-6\\_8](http://link.springer.com/content/pdf/10.1007%2F3-540-33133-6_8). 2.4.2
- [Weedbrook et al., 2004] Weedbrook, C., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C., and Lam, P. K. (2004). Quantum Cryptography Without Switching. *Phys. Rev. Lett.*, 93:170504. 2.2.1
- [Weier, 2003] Weier, H. (2003). Experimental Quantum Cryptography. Master’s thesis, Physik Department. Technische Universität München (Germany). [http://www.xqp.physik.uni-muenchen.de/publications/files/theses\\_diplom/diplom\\_weier.pdf](http://www.xqp.physik.uni-muenchen.de/publications/files/theses_diplom/diplom_weier.pdf). 2.4.3
- [Weier, 2011] Weier, H. (2011). *European Quantum Key Distribution Network*. PhD thesis, Faculty of Physics. Ludwig Maximilians Universität, München (Germany). [http://edoc.ub.uni-muenchen.de/13320/1/Weier\\_Henning.pdf](http://edoc.ub.uni-muenchen.de/13320/1/Weier_Henning.pdf). 2.4.3
- [Weier et al., 2006] Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C., and Weinfurter, H. (2006). Free space quantum key distribution: Towards a real life application. *Fortschr. Phys.*, 54:840–845. [http://www.xqp.physik.uni-muenchen.de/publications/files/proceedings\\_books/fortschrphys\\_54\\_840.pdf](http://www.xqp.physik.uni-muenchen.de/publications/files/proceedings_books/fortschrphys_54_840.pdf). 6.3.4
- [Weier et al., 2011] Weier, H., Krauss, H., Rau, M., Fürst, M., Nauerth, S., and Weinfurter, H. (2011). Quantum Eavesdropping without Interception: An Attack Exploiting the Dead Time of Single-Photon Detectors.

- New Journal of Physics*, 13(7):073024. <http://arxiv.org/pdf/1101.5289.pdf>. 2.4.3
- [Weihs et al., 2007] Weihs, G. and Erven, C. (2007). Entangled free-space quantum key distribution. In *Proceedings of SPIE 6780, Quantum Communications Realized*, pages 678013–678013–9. <http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=825444>. 2.5
- [Weinfurter, 2005] Weinfurter, H. (2005). From EPR to quantum computing: experiments on entangled quantum systems. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 38(9):S579. 2.3.1
- [Wiechers et al., 2011] Wiechers, C., Lydersen, L., Wittmann, C., Elser, D., Skaar, J., Marquardt, C., Makarov, V., and Leuchs, G. (2011). After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1):013043. <http://www.vad1.com/publications/NewJPhys-13-013043.pdf>. 2.4.3
- [Wiesner, 1983] Wiesner, S. (1983). Conjugate coding. *ACM SIGACT News*, 15(1):78–88. 2.1.4
- [Willebrand et al., 2002] Willebrand, H. and Ghuman, B. S. (2002). *Free-Space Optics: Enabling Optical Connectivity in Today's Networks*. SAMS Publishing. ISBN: 067232248X, Indianapolis, Indiana (USA). 2.3.2, 4.1
- [Wootters et al., 1982] Wootters, W. and Zurek, W. (1982). A single quantum cannot be cloned. *Nature*, 299:802–803. (document), 1.1, 2.1.4
- [Xu et al., 2010] Xu, F., Qi, B., and Lo, H.-K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026. <http://arxiv.org/pdf/1005.2376.pdf>. 2.4.3
- [Yuan et al., 2008] Yuan, Z., Dixon, A., Dynes, J., Sharpe, A., and Shields, A. (2008). Gigahertz quantum key distribution with InGaAs avalanche photodiodes. *Applied Physics Letters*, 92(20):201104–201104–3. <http://arxiv.org/pdf/0805.3414v1.pdf>. 1.1, 3.3.2

- [Yuan et al., 2011a] Yuan, Z. L., Dynes, J. F., and Shields, A. J. (2011). Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. *Appl.Phys.Lett.*, 98:231104. <http://arxiv.org/pdf/1106.2675v1>. 2.4.3
- [Yuan et al., 2011b] Yuan, Z. L., Dynes, J. F., and Shields, A. J. (2011). Response to Comment on “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography”. *Applied Physics Letters*, 99:196102–1–196102–2. <http://www.vad1.com/publications/ApplPhysLett-99-196102.pdf>. 2, 2.4.3, 2.4.3, 2
- [Zbinden et al., 1997] Zbinden, H., Gautier, J. D., Gisin, N., Huttner, B., Muller, A., and Tittel, W. (1997). Interferometry with Faraday mirrors for quantum cryptography. *Electronics Letters*, 33(7):586–588. <http://arxiv.org/pdf/quant-ph/9703024v1>. 2.3.2
- [Zbinden et al., 1998] Zbinden, H., Bechmann-Pasquinucci, H., Gisin, N., and Ribordy, G. (1998). Quantum cryptography. *Appl. Phys. B*, 67:743–748. [http://www.gap-optic.unige.ch/wiki/\\_media/publications:bib:80670743.pdf](http://www.gap-optic.unige.ch/wiki/_media/publications:bib:80670743.pdf). 2.2.2
- [Zhao et al., 2008a] Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C., and Lo, H.-K. (2008). Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333. <http://arxiv.org/pdf/0704.3253v3.pdf>. 2.4.3
- [Zhao et al., 2008b] Zhao, Y., Qi, B., and Lo, H.-K. (2008). Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A*, 77:052327. <http://arxiv.org/pdf/0802.2725v3.pdf>. 2.4.3



# Glossary

Term	Meaning
AES	Advanced Encryption Standard
APC	Automatic Power Control
APD	Avalanche Photo Diode
AQC	Active Quenching Circuit
B92	Bennet, 1992
BB84	Bennet and Brassard, 1984
BBM	Bennett, Brassard, Mermin, 1992
BS	Beam-Splitting
BSC	BeamSplitter Cube
CA	Certificate Authority
COW	Coherent One Way
DBR	Distributed Bragg Reflector
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DH	Diffie-Hellman
DIQKD	Device-Independent Quantum Key Distribution
DPS	Differential Phase Shift
E91	Ekert, 1991
EV	Evaluation Kit
FM	Faraday Mirror
FWHM	Full Width at Half Maximum
FW10%M	Full Width at 10th Maximum
FW1%M	Full Width at 100th Maximum
GIS	Geographic Information System
GSM	Global System for Mobile communications
IF	Interference Filter
LOS	Line Of Sight
MPD	Micro Photon Devices
NbN	Niobium Nitride

Term	Meaning
NEP	Noise Equivalent Power
NRZ	Non-Return-to-Zero
QBER	Quantum Bit Error Rate
QC	Quantum Cryptography
QDS	Quantum Digital Signatures
QKD	Quantum Key Distribution
OSA	Optical Spectral Analyser
PBS	Pellicle Beam Splitter
PD	Photodetector
PDJ	Pattern Dependent Jitter
PER	Polarisation Extinction Ratio
PMT	PhotoMultiplier Tubes
PNS	Photon-Number Splitting
PPG	Pulse Pattern Generator
PRBS	Pseudo-Random Bit Sequence
QDS	Quantum Digital Signatures
RNG	Random Number Generator
SAM APD	Separate-Absorption-Multiplication APD
SARG04	Scarani, Acin, Ribordy, Gisin, 2004
Si-SPAD	Silicon Single-Photon Avalanche Diode
SPAD	Single-Photon Avalanche Diode
SPCM	Single-Photon Counting Module
SPD	Single-Photon Detector
SSPD	Superconducting Single-Photon Detectors
TDEA	Triple DEA
TIA	Time Interval Analyser
USD	Unambiguous State Discrimination
VCSEL	Vertical-Cavity Surface-Emitting Laser
WCP	Weak Coherent Pulses
XOR	eXclusive-OR



# Alphabetical index

- Absorption, 97
- Afterpulsing probability, 67
- Alberti's disc, 22
- Alignment, 111
- Atmospheric extinction, 91
- Attack
  - after-gate, 53
  - blinding, 51
  - bright illumination, 51
  - channel calibration, 48
  - collective, 54
  - dead time, 52
  - faked states, 50
  - fixed apparatus, 53
  - intercept-resend, 46, 53
  - large pulse, 48
  - memory, 55
  - optimal eavesdropping, 47
  - passive faraday mirror, 53
  - phase-remapping, 48
  - photon-number splitting, 48
  - quantum cloning, 47
  - reversed-space, 53
  - thermal blinding, 52
  - time-shift, 50
  - Trojan-horse, 49
  - USD, 46
- Attenuation, 101
- Avalanche breakdown voltage, 124
- Background radiation, 44, 136
- Background rate, 154
- Beam divergence, 104
- Beam spreading, 99, 100, 161
- Beam wander, 99, 137, 149, 161
- Beer's Law, 95
- Bias current, 67
- Binary entropy function, 147
- Bit-mapped gating, 50
- Block ciphers
  - AES, 26
  - DEA, 26
  - DES, 26
  - TDEA, 26
- Bragg reflector, 65
- Cascade, 37
- Cipher, 20
  - block, 26
  - Caesar, 21
  - homophonic, 24
  - monoalphabetic, 21
  - one-time pad, 24
  - polyalphabetic, 22
  - substitution, 21
  - transposition, 21
  - Vernam, 24
  - Vigenère, 22

- Ciphertext, 20  
Collimation, 103  
Cryptogram, 20  
Cryptography, 20  
    asymmetric, 27  
    public key, 27  
    secret key, 25  
    symmetric, 25  
Cryptosystem, 20  
  
Dark counts, 44  
Dark-count rate, 50  
Decoy states, 49  
Decryption, 20  
Detection loophole, 55  
Device-independent QKD, 54  
Distributed Bragg Reflector, 65  
  
Eavesdropping, 33  
Edge-emitting laser, 65  
Encryption, 20  
Error correction, 33, 150  
Extinction ratio, 69  
  
Faraday mirror, 49, 53  
Frequency analysis, 21  
  
Gating frequency, 138  
Gaussian beam, 103  
Geiger mode, 124  
Geometrical loss, 94  
  
Impact ionisation, 124  
Interference filter, 136  
Intersymbol interference, 43  
  
Jitter, 64, 149  
  
Kerckhoff's principle, 29  
Key, 25  
    raw key, 33  
  
Line of sight, 92  
Loophole, 47, 166  
  
Mie scattering, 96  
Misalignment, 94, 156  
MODTRAN, 98  
Modulation current, 67  
Multimode fibre, 69  
  
Net bit rate, 149  
No-cloning theorem, 30  
Noise equivalent power, 119  
  
Optical loss, 94  
Optical path, 106  
  
Parametric downconversion, 39  
Pattern dependent jitter, 71  
Photodetector, 139  
Plaintext, 20  
Pointing loss, 94  
Polarisation extinction ratio, 78, 158  
Polarisation leakage, 78, 131, 158  
Polarisation state, 32  
Privacy amplification, 33, 37, 147, 150  
Public key cryptography  
    DH, 27  
    RSA, 27  
Pulse pattern generator, 73  
  
QBER, 53, 73, 154  
    contributions, 157  
QKD, 19  
    plug and play, 40, 48

- protocols
  - B92, 31
  - BB84, 31
  - BBM, 31
  - continuous-variable, 31
  - COW, 31
  - differential phase shift, 49
  - discrete-variable, 31
  - distributed-phase-reference, 31
  - DPS, 31
  - E91, 31
  - entangled states, 31
  - non-orthogonal states, 31
  - SARG04, 31, 49
  - six-state, 31
- Quantum channel, 91
- Quantum conjugate coding, 30
- Quantum key distribution, 30
- Quantum states, 43, 92, 147
- Qubit, 30
- Quenching, 124
- Rayleigh scattering, 96
- Receiver, 116
  - loss, 131
- Refractive index structure constant, 161
- Repetition rate, 149
- Scintillation, 100
- Secret key rate, 144, 145
- Side channel attack, 45
- Sifted bit rate, 149
- Signal amplification, 135
- Single-photon detectors, 50
- Skytale, 20
- Spatial filtering, 137
- Spectral filtering, 136
- Stability, 153
- Superlinear threshold detector, 53
- Synchronisation signal, 116
- Test events, 33
- Threshold current, 65
- Time interval analyser, 73, 116, 127
- Timing jitter, 121
- Trans-impedance amplifier, 139
- Transmitter, 61
- Turbulence, 99
  - regimes, 161
- VCSEL, 63, 68, 136
- Weak coherent pulses, 64